



WLINK

User Manual

---Apply to WL-R100/R130/R200/R210/R230/R520

Series 4G/3G Router

V3.7

<http://www.wlink-tech.com>

Jan 2026



Copyright © Shenzhen WLINK Technology Company Limited 2012 ~ 2026

Without our written approval, anyone can't extract, copy whole or part of content of this file and can't spread out in any format.

Caution

Due to product updates or functional upgrading, we may renew the content of this file, and this file only for reference. All statement, information, suggestion etc. in this file does not compose any form of guarantee and we WLINK reserves the right of final explanation.

Version History

Updates between document versions are cumulative. The latest document version contains all updates made to previous version.

Data	Document Version	Firmware Version	Description
2026-1-22	V3.7	Rm.0.2.7-250806-100643.bin	Improved VLAN Improved Modbus
2025-1-2	V3.6	Rm.0.2.7-241225-103101.bin	Added Zerotier VPN. Add OpenVPN Server. Improved link backup feature Improved ICMP Check
2024-3-20	V3.5	Rm.0.2.6-240318-093407.bin	Improved 4G/WAN backup. Added Wireguard Feature.
2023-1-5	V3.4	Rx_4.3.4.6_22-10-21.trx	Improved DDNS.
2022-1-6	V3.3	Rx_4.3.4.5_22-01-06.trx	Improved Serial App, reset default, M2M connection. Added MTU Setting.
2021-4-2	V3.1	Rx_4.3.4.5_21-03-22.trx	Improved the scheduled reboot
2020-8-1	V3.0	Rx_4.3.4.5_20-07-29.trx	Upgrade UI from 2.0 to 3.0

Shenzhen WLINK Technology Company Limited

Add 2A, F5 Building, TCL International E City, No.1001 Zhongshanyuan Rd.,
Nanshan Dist., Shenzhen, 518052, China

Web <http://www.wlink-tech.com>

Service Email support@wlink-tech.com

Tel 86-755-86089513

Fax 86-755-26059261

Contents

1 Hardware Introduction	5
1.1 WL-Rxx Family List	5
1.2 LED Indicator	6
1.3 Serial Port Connection	7
1.4 Power Supply	7
1.5 Review	7
2 Router Configuration	8
2.1 Local Configure	8
2.2 Status	9
2.3 Overview	9
2.4 Traffic Stats	10
2.5 Device List	10
2.6 Tool Column	11
2.7 Basic Network	13
2.8 WLAN Setting	24
2.9 Advanced Network Setting	26
2.10 Firewall	37
2.11 VPN Tunnel	39
2.12 Administration	59
3 Configuration Instance	74
3.1 VLAN	74
3.2 WAN Backup (WAN as Main, Cellular Backup)	76
3.3 Port Forwarding	78
3.4 Port Redirecting	79
3.5 IP Passthrough	80
3.6 Captive Portal	85
3.7 GPS Settings	88

3.8 Firewall	91
3.9 VPN Tunnel	92

1 Hardware Introduction

This chapter is mainly for hardware introduction, there would be some difference between the scheme and real object. But the difference won't have any influence to products performance.

1.1 WL-Rxx Family List

Model	Appearance	SIM Card	LAN	WAN	Wi-Fi	Serial Port	I/O	USB	Dimension(mm)
WL-R100		One	One	N/A	N/A	RS232	N/A	N/A	78.5x59x23.5
WL-R130		Two	One	N/A	Optional	RS232 RS485	N/A	N/A	103x73.5x25.5
WL-R200		One	Two	Optional	Optional	N/A	N/A	N/A	103x73.5x25.5
WL-R210		Two	Two	One	Default	RS232	2*DI 1*DO	N/A	102x100x42
WL-R230		Two	Two	One	Default	RS232 RS485	2*DI 1*DO	One	102x100x42
WL-R520		Two	Four	One	Default	RS232	N/A	NA	176x105x25

1.2 LED Indicator

1) WL-R100/R130/R200/R520 LED Status

silk-screen	color	status	Indication
NET	Red		Pool Signal
	Green		Strong Signal
		Solid light	4G Online
		Slow Blink (1.5s)	3G Online
		Quick Blink (0.5s)	Offline
LAN(WAN)	Green	Solid light	Plugged
	Green	Blinking	Data Sending
	Green	Dark	Unplugged
PWR	Green	Solid light	Router OS is running.

2) WL-R210/R230 LED Status

silk-screen	status		Indication
Signal	Signal LED	Solid Light	LED1 indicates signal is Pool (CSQ0~10) LED2 indicates signal is good (CSQ11~19) LED3 indicates signal is strong (CSQ20~31)
		Quick Blink	Offline
	LED 1	Solid Light	4G Online
		Slow Blink	3G Online
PWR	Solid Light		System power operation.
WLAN	Solid light		WLAN enable, but no data communication.
	Quick Blinking		Data Send
	Dark		WLAN disable
ERR	Dark		System operation and LTE/3G online.
	Solid Light (Red)		System fail indicator such as SIM card/ module fail.
LAN(WAN)	Green	Solid light	Plugged
	Green	Blinking	Data in transmitting.
	Green	Dark	Unplugged

1.3 Serial Port Connection

The serial port supports alternative RS232/RS485 port, and RS232 port as default. It might be requested serial port for RS485 when place order. The serial port feature supports TCP/UDP client/server as optional, also supports Modbus protocol. You may check the feature in Serial App of Advanced Network UI.



WL-R200 series doesn't support serial port feature in hardware as default.

1.4 Power Supply

Voltage input range: +7.5~32VDC. (R230 input range: 9~ 60VDC)

1.5 Review

After insert the SIM/UIM card and connect Ethernet cable and antenna, connect power supply adaptor or power cable.



Please connect the antenna before power on, otherwise the signal maybe poor because of impedance mismatching.

Notice:

- Step 1 Check the antenna connection.
- Step 2 Check SIM/UIM card, confirm SIM/UIM card is available.
- Step 3 Power on the industrial Router

----END

2 Router Configuration

WL-Rxx Series routers support GUI and CLI configuration. This chapter introduce GUI configuration via Ethernet port, if need CLI configuration guide, please contact our technical support department by email: support@wlink-tech.com.

2.1 Local Configure

The router supports to be configured by local Ethernet port, you could specify a static IP or set as DHCP. The default IP address is 192.168.1.1, subnet mask is 255.255.255.0, please refer to following.

Step 1 Click “start > control panel”, find “Network and Internet” and click it, select “Network and Sharing Center” corresponding to the network card on this page. Refer to the figure below.

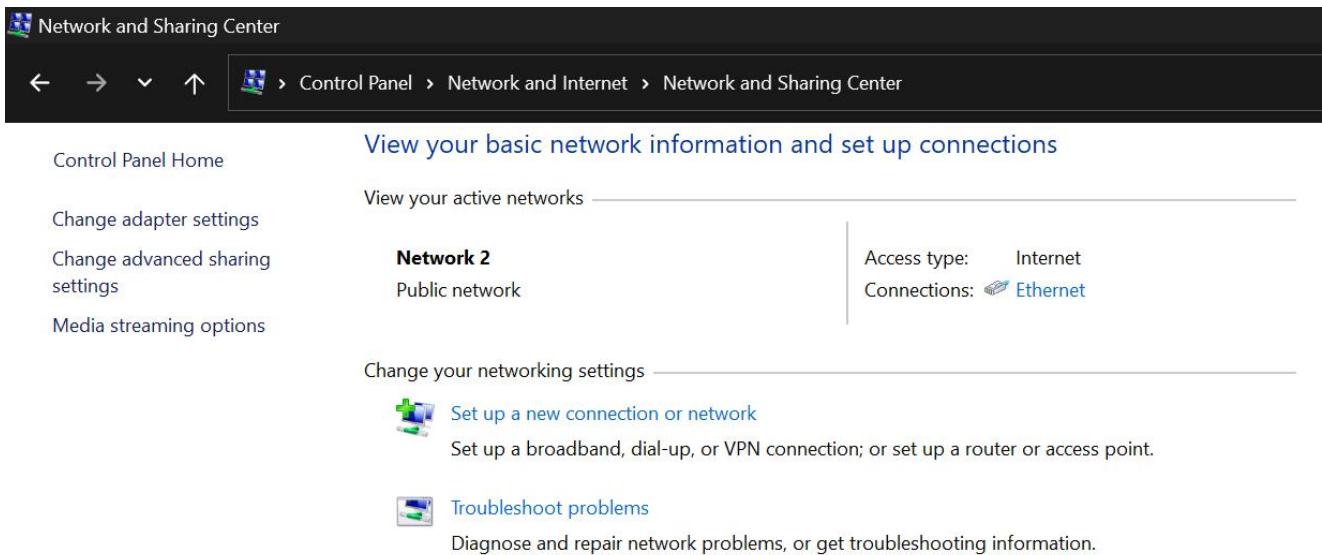


Figure 2-1 Network Connection

Step 2 Obtain a IP address automatically or set up IP address,192.168.1.xxx(XXX can be any number between 2~254)

Step 3 Run an Internet Explorer and visit “<http://192.168.1.1/>”, to enter identify page.

User should use the default username and password when log in for the first time.

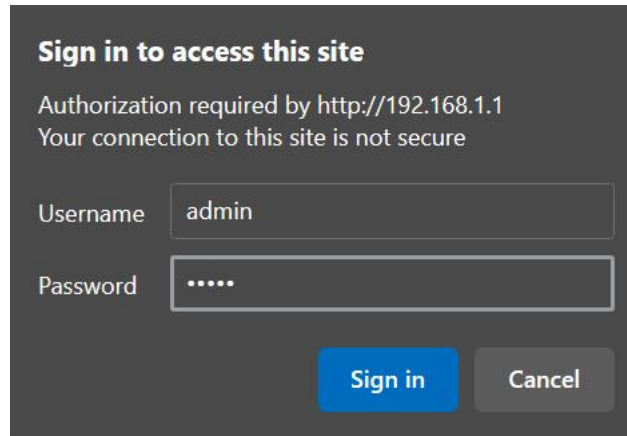


Figure 2-2 User Identify Interface

----END

2.2 Status

Check routers information such as status, traffic Stats and device list after login router. Especially, suggest change the password according to the prompts because of security requirement.

You haven't changed the default password for this router. To change router password [click here](#).

The UI will display "already changed login password successfully" after router reboot.

Already changed login password successfully.

2.3 Overview

The overview GUI will be display router system information, Ethernet ports status, VPN connection status, LAN information, 4G connection information and WLAN information.

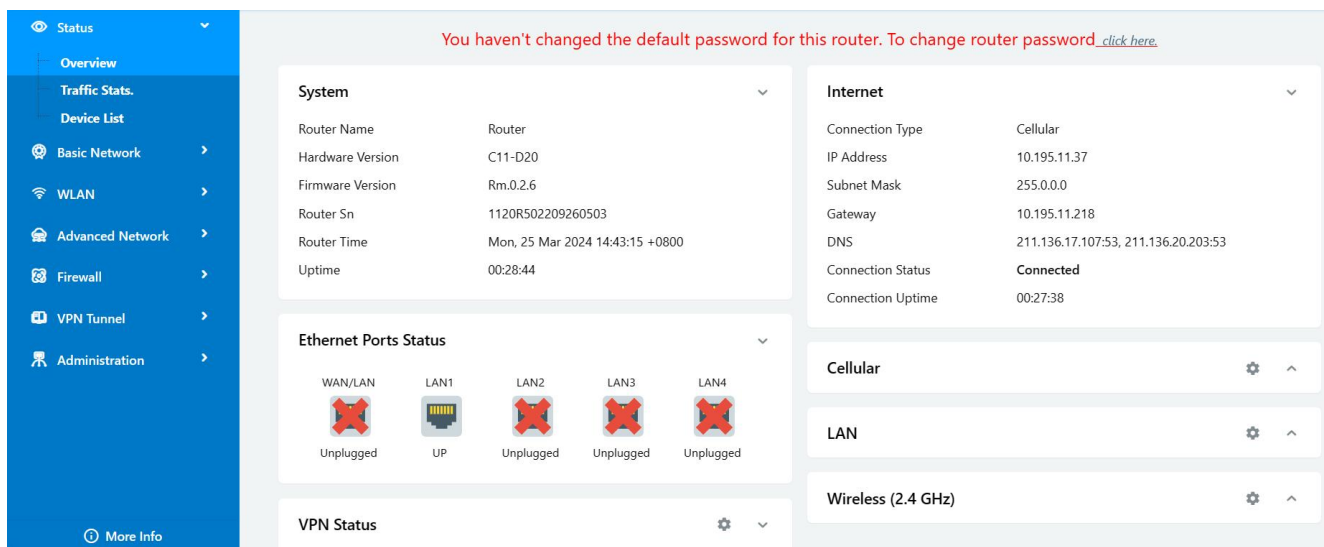


Figure 2-3 Router Status GUI



One Ethernet Port Icon for WL-R100, R130.
 Two Ethernet Port Icons for WL-R200 and WL-R210.
 Three Ethernet Port Icons for WL-R230.
 Five Ethernet Port Icons for WL-R520.

2.4 Traffic Stats.

Click Status->Traffic Stats. to enter the traffic stats.GUI to check Cellular/WAN traffic in real-time.

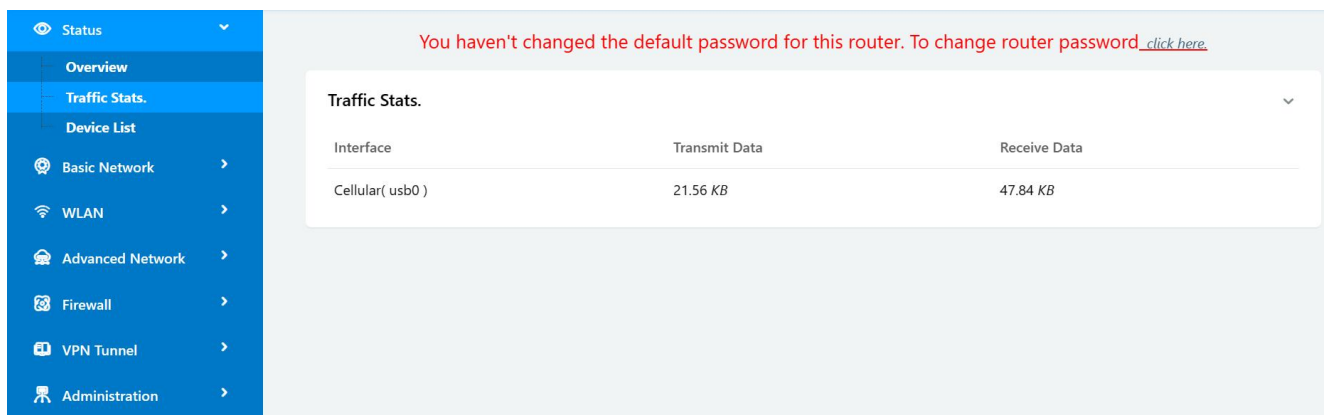


Figure 2-4 Traffic Stats. GUI

2.5 Device List

Click Status->Device List to enter the device list GUI to check the connected devices information in the list.

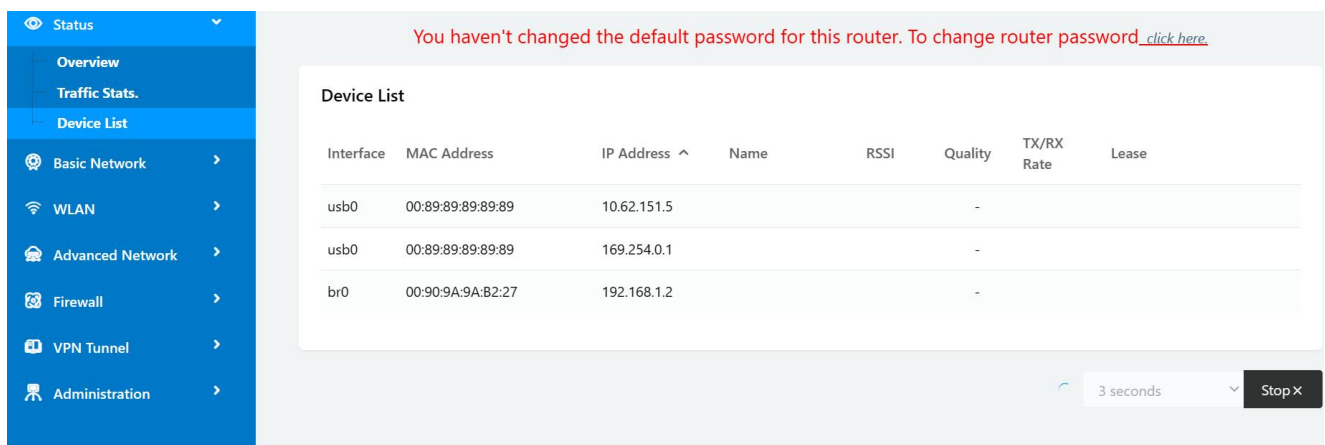


Figure 2-5 Device List GUI

2.6 Tool Column

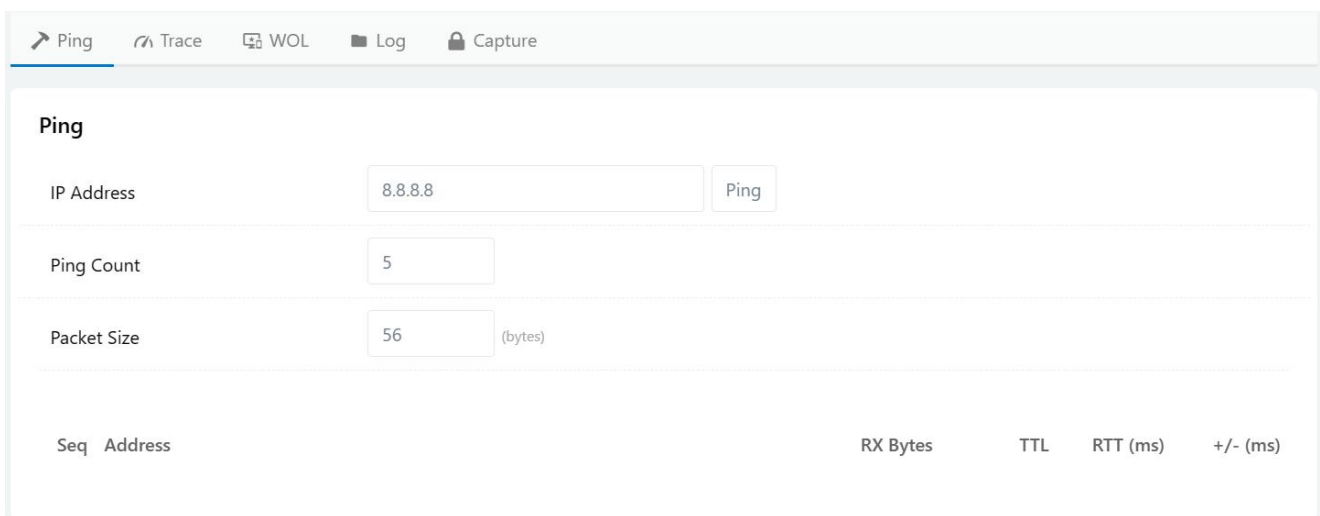


Figure 2-6 Tool Column GUI

2.6.1 Tools

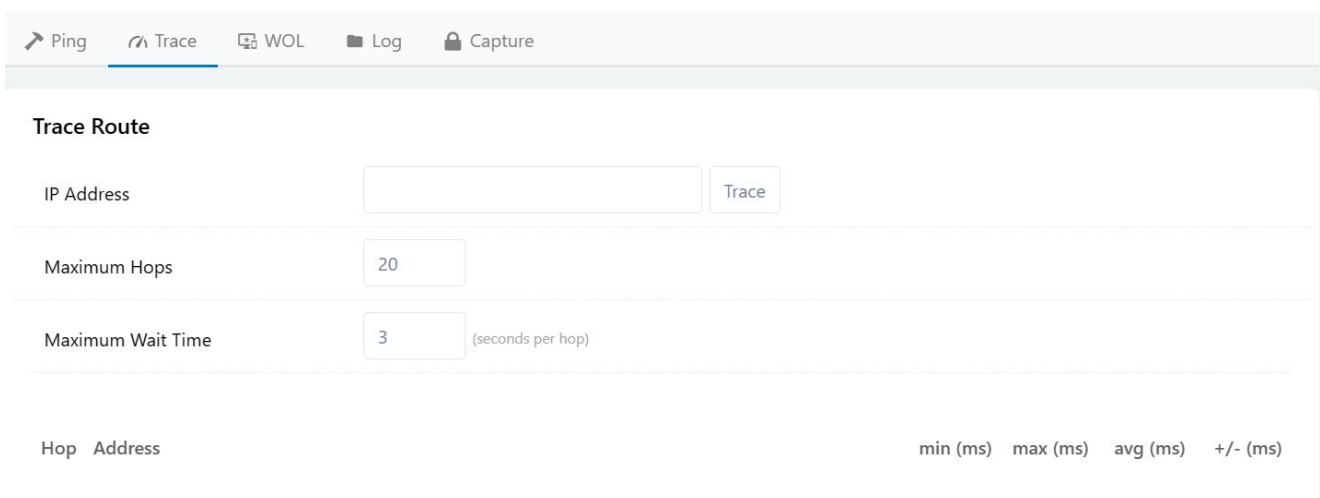
2.6.1.1 Ping

Click Tools->Ping to enter ping test GUI. Used to test the reachability of a host on an Internet IP network and to measure the round-trip time for messages sent from the originating host to a destination server.



2.6.1.2 Trace

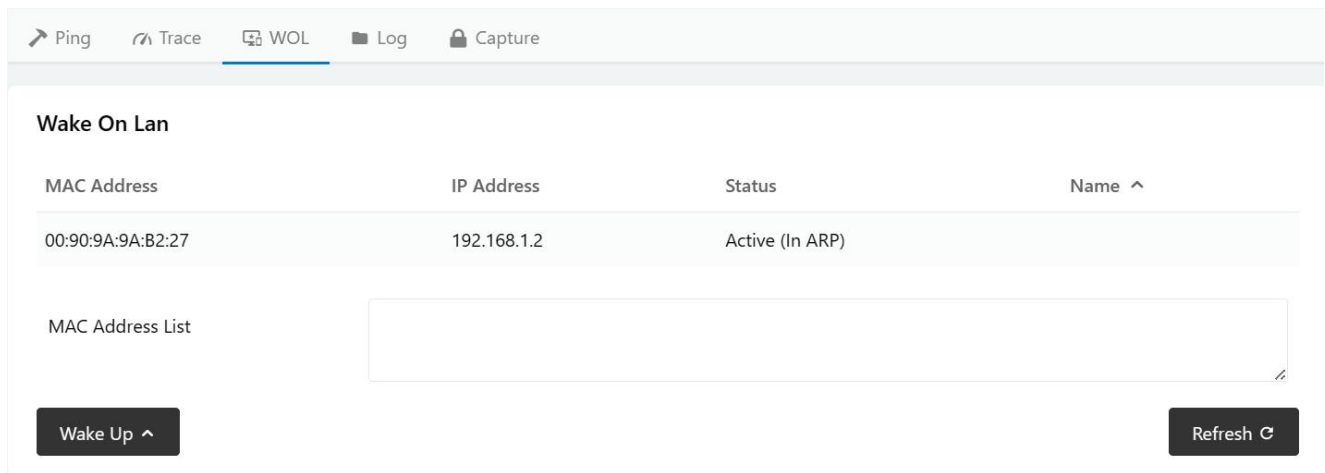
Click Tools->Trace to enter trace test GUI. diagnostic tool for displaying the route and measuring transit delays of packets across an Internet IP network.



2.6.1.3 WOL

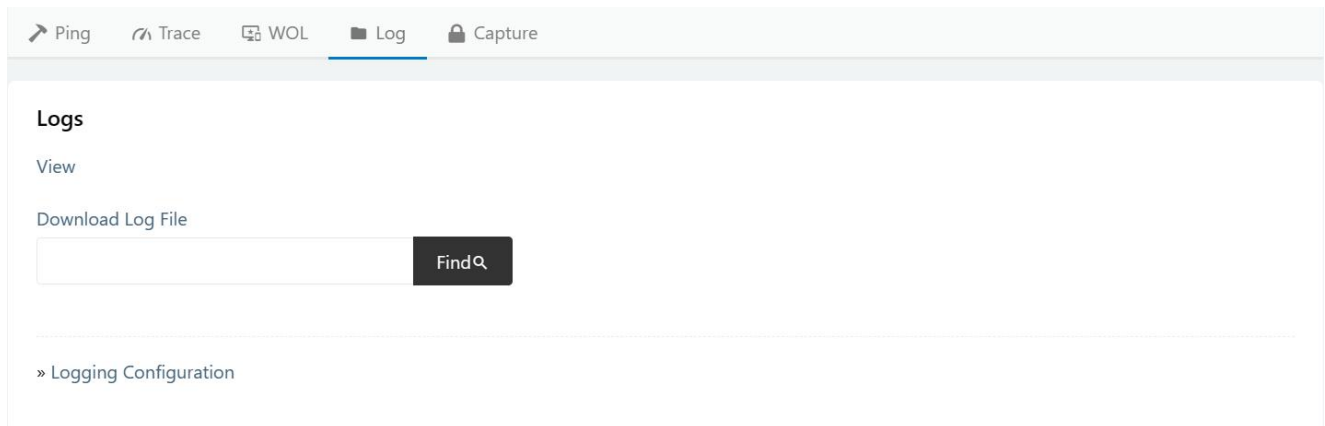
Click Tools-> WOL to enter WOL(Wake On Lan) GUI. Used to wake up those connected devices via WOL protocol.

Click left mouse button to wake up the device.



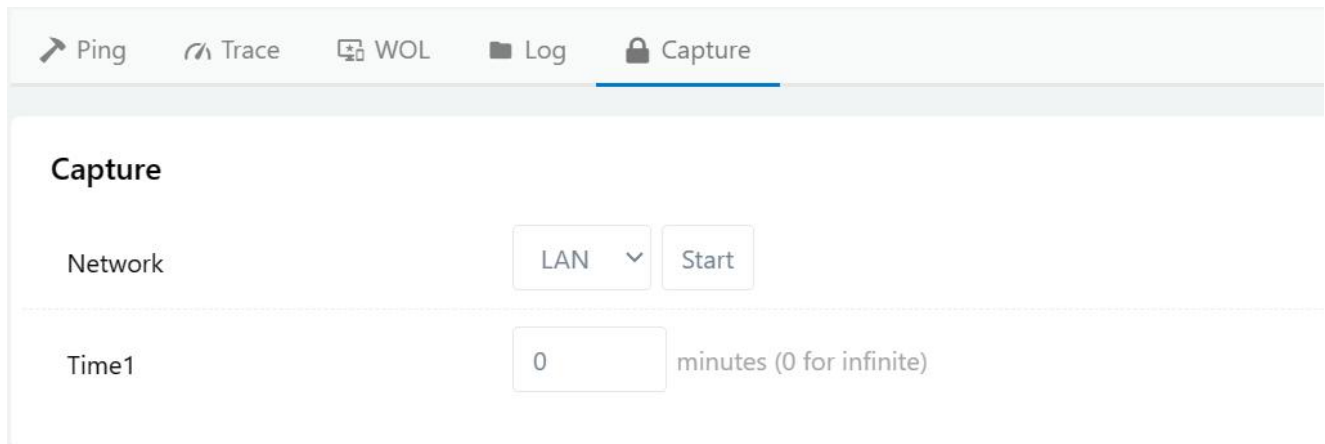
2.6.1.4 Log

Click Tools-> Log to enter Log GUI. Use to check logs in GUI, download GUI and send logs to server.



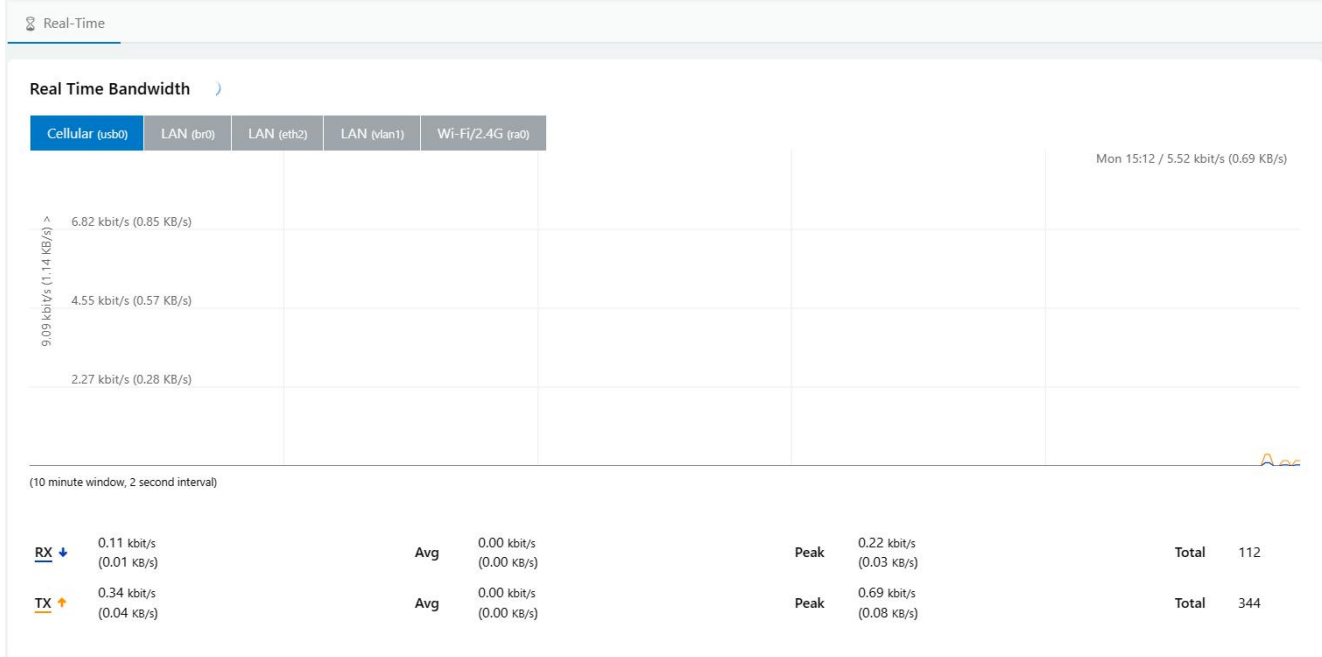
2.6.1.5 Capture

Click Tools-> Capture to enter capture data GUI. Use to capture LAN/WAN data packet to analyse what happen in the router.



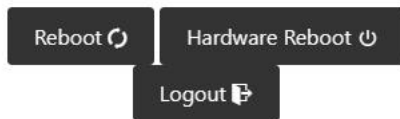
2.6.2 Bandwidth

Click Bandwidth to enter bandwidth graphic GUI. Used to check cellular/LAN/Wi-Fi real-time bandwidth.



2.6.3 System

Click system to choose software reboot, hardware reboot and logout GUI.



2.7 Basic Network

2.7.1 WAN Setting

Step 1 Basic Network>WAN to enter below interface.

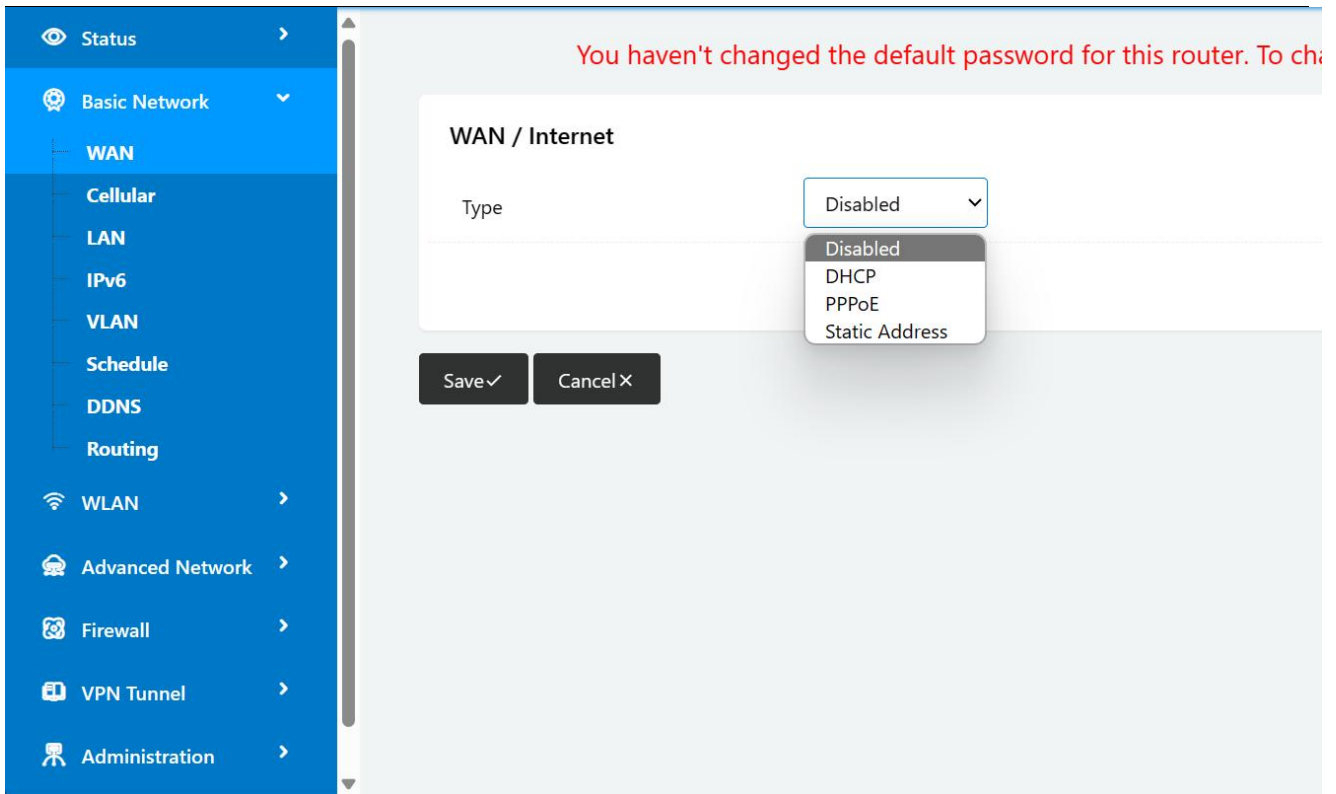


Table 2-1 WAN Setting Instruction

Parameter	Instruction	Default
Type	Support DHCP, PPPoE, Static IP address	Disable

Step 2 After setting, please click “save” to finish, the device will reboot.

----End

2.7.2 Cellular Setting

Step 1 Basic Network-> Cellular, you can modify relevant parameter according to the application.

The screenshot shows the 'Cellular Settings' page in the router's web interface. The left sidebar contains a navigation menu with 'Cellular' selected under the 'WAN' section. The main content area is titled 'Cellular Settings' and features a toggle for 'Enable Modem' which is checked. Below this, there are tabs for 'Basic Settings', 'SIM 1', and 'SIM 2'. The 'Basic Settings' tab is active and contains the following configuration options:

- IMS:
- Use PPP:
- ICMP Check:
- Cellular Traffic Check:
- MTU: (0 for default)
- CIMI Send to: :
- SMS Code:
- Operator Lock: *ex:46001*
- DualSim Mode:

The screenshot shows the 'Cellular Settings' page in the router's web interface, specifically the 'SIM 1' configuration tab. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Cellular Settings' and features a toggle for 'Enable Modem' which is checked. Below this, there are tabs for 'Basic Settings', 'SIM 1', and 'SIM 2'. The 'SIM 1' tab is active and contains the following configuration options:

- SIM 1 Mode:
- SIM 1 Network Operator:
- SIM 1 PIN Code:
- SIM 1 APN:
- SIM 1 User:
- SIM 1 Password:
- SIM 1 Dial Number:
- SIM 1 Auth Type:
- SIM 1 Local IP Address:



WL-R100 supports single SIM.
 WL-R200/R520 supports dual-SIM as optional.
 WL-R130/R210/R230 supports dual-SIM as default.

Table 2-2 Cellular Setting Instruction

Parameter	Instruction	Default
Enable Modem	Enable/Disable 4G mode.	Enable
Use PPP	ECM dialup as default. PPP optional.	Disable
ICMP check	If enable ICMP check and setup a reachable IP address as destination IP, the router will reconnect/reboot once ICMP check failed.	
Cellular Traffic Check	The router will reconnect/reboot once there's no Rx/Tx data.	
CIMI Send to	Send CIMI to a defined IP and port by TCP protocol.	
SMS Code	Remote control the router by SMS. Only the configured SMS code will work.	
Operator Lock	Lock a specified operator for the router by MCC/MNC code.	
Dual SIM Mode	<p>【Fail Over】Two SIM cards mutual backup. Once SIM1 failed, it'll switch to SIM2 and work on SIM2, and vice versa.</p> <p>【SIM1 Only】 Only SIM1 works.</p> <p>【SIM2 Only】 Only SIM2 works.</p> <p>【Backup】 SIM1 is the primary SIM. Once SIM1 failed, it'll switch to SIM2 and work on SIM2 for a specified period of time, then it switches back to SIM1.</p>	
Connect Mode	<p>【Auto】 The router will automatically connect to 3G/4G networks and give priority to 4G.</p> <p>【LTE】 Router will connect to 4G only.</p> <p>【3G】 Router will connect to 3G only.</p>	
Pin Code	Some SIM cards are locked with a Personal Identification Number (PIN) code in case they are lost or stolen.	
APN	APN is provided by local ISP, usually CDMA/EVDO networks do not need this parameter.	
User	SIM card username is provided by ISP	
Password	SIM card password is provided by ISP	
Auth Type	Auto/PAP/Chap/MS-Chap/MS-Chapv2 authentication optional.	
SIM Local IP Address	Fix SIM IP. The feature is available if carrier can provide this service.	



NOTE ICMP Check and Cellular Traffic Check are alternative.

【ICMP Check】

Enable ICMP, Router will automatically check whether the defined IP address is reachable per 60s. If the IP address is unreachable and ICMP check is timeout at the first time, it will check 2 times every 3 seconds. If the third time is still failed, the router will redial.

The ICMP Check IP is a public IP or company server IP address.

ICMP Check	<input checked="" type="checkbox"/>
Check IP	<input type="text" value="8.8.8.8"/>
Check IP (Optional)	<input type="text" value="8.8.4.4"/>
Interval	<input type="text" value="60"/> (seconds)
Retries	<input type="text" value="3"/> (Times)
ICMP RTT Enable	<input type="checkbox"/>
Fail Action	Reboot System <input type="button" value="v"/>

【Cellular Traffic Check】

【Check Mode】 there are Rx(Receive), Tx(Transmission) and Rx/Tx check modes.

【Rx】 Router will check the 3G/LTE cellular receiver traffic. If no receiver traffic within the defined check interval, the router will implement the specified action reconnect or reboot.

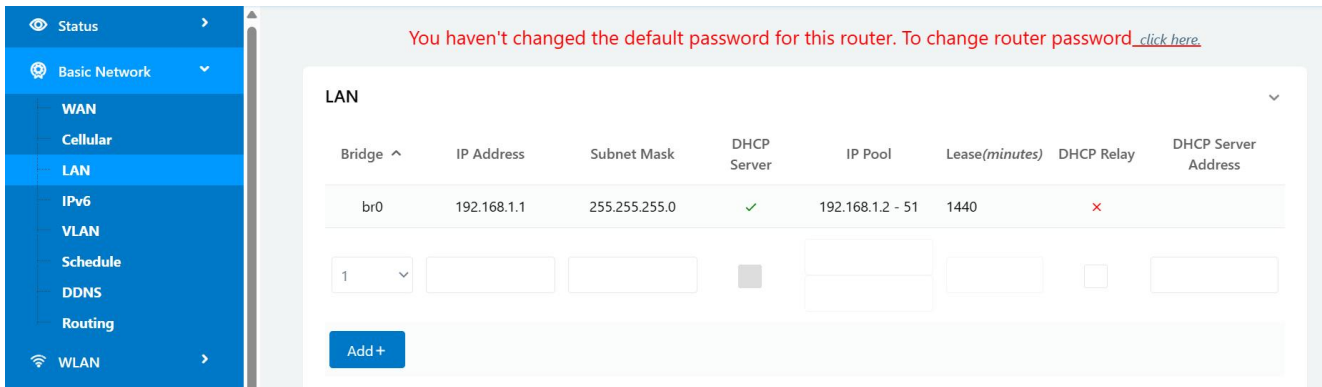
Cellular Traffic Check	<input checked="" type="checkbox"/>
Check Mode	Rx <input type="button" value="v"/>
Check Interval	<input type="text" value="10"/> (minutes)Range: 1 ~ 1440
Fail Action	Cellular Reconnect <input type="button" value="v"/>

Step 2 After Setting, please click “save” icon.

----End

2.7.3 LAN Setting

Step 1 Basic Network>LAN to enter below interface



Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)	DHCP Relay	DHCP Server Address
br0	192.168.1.1	255.255.255.0	✓	192.168.1.2 - 51	1440	✗	

1 ▾ [] [] [] [] [] [] []

Add +

Table 2-3 LAN Setting Instruction

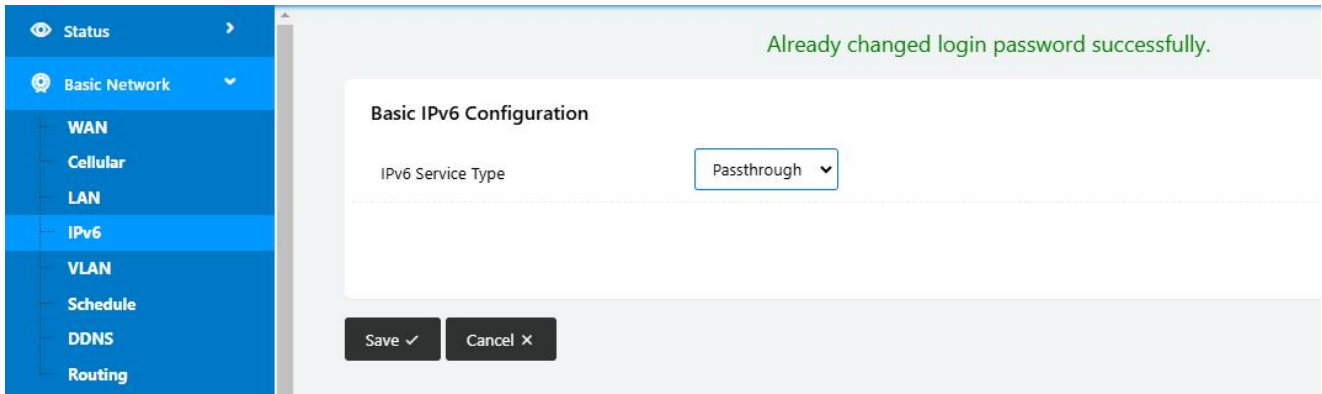
Parameter	Instruction	Default
Bridge	Supports 4 LAN IP address for br0 to br3 interface. If need to support VLAN, please go to VLAN GUI.	
Router IP Address	Router IP address, default IP is 192.168.1.1	192.168.1.1
Subnet Mask	Router subnet mask, default mask is 255.255.255.0	255.255.255.0
DHCP	Dynamic allocation IP service, after enable, it will show the IP address range and options of lease	Enable
IP Pool	IP address range within LAN	192.168.1.2—51
Lease	The valid time, unit as minute	
Add	Add LAN IP address, supports 4 LAN IP addresses.	

Step 2 After setting, please click “save” to finish, the device will reboot.

----End

2.7.4 IPv6

Step 1 Basic Network->IPv6 to enter the IPv6 setting page.



Step 2 Please Click “Save” to finish.

----End

2.7.5 VLAN

Step 1 Basic Network->VLAN to enter the VLAN setting page.

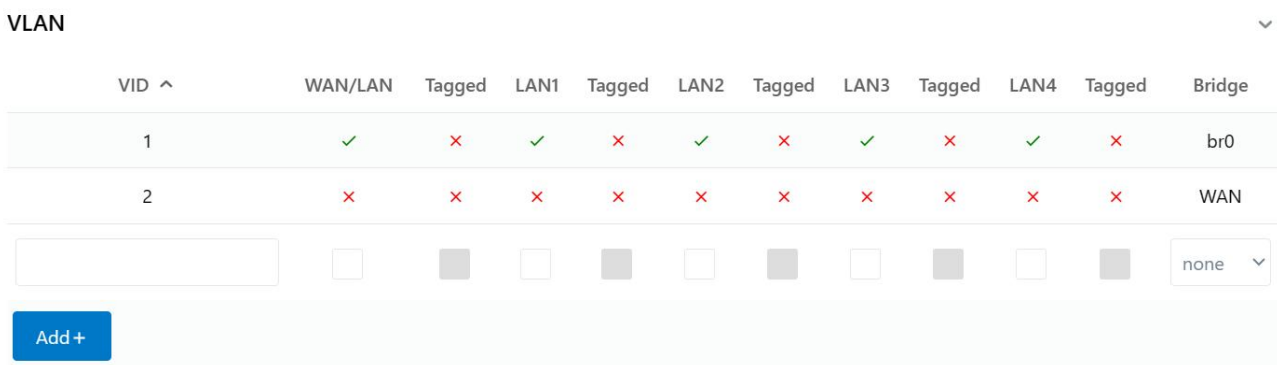


Table 2-4 LAN Setting Instruction

Parameter	Instruction	Default
VID	VLAN ID number. The VID range is from 1 to 15.	
LAN1~LAN4, WAN	LAN	
Tagged	Enable to make router can encapsulate and de-encapsulate the VLAN tag.	
Bridge	Routers interface br0, br1, br2, br3 and WAN	

Step 2 Please Click “Save” to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

2.7.6 Schedule

Step 1 Basic Network->VLAN to enter the Schedule setting page.

Step 2 Please Click “Save” to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

2.7.7 Dynamic DNS Setting

Step 1 Basic Network->DDNS to enter the DDNS setting page.

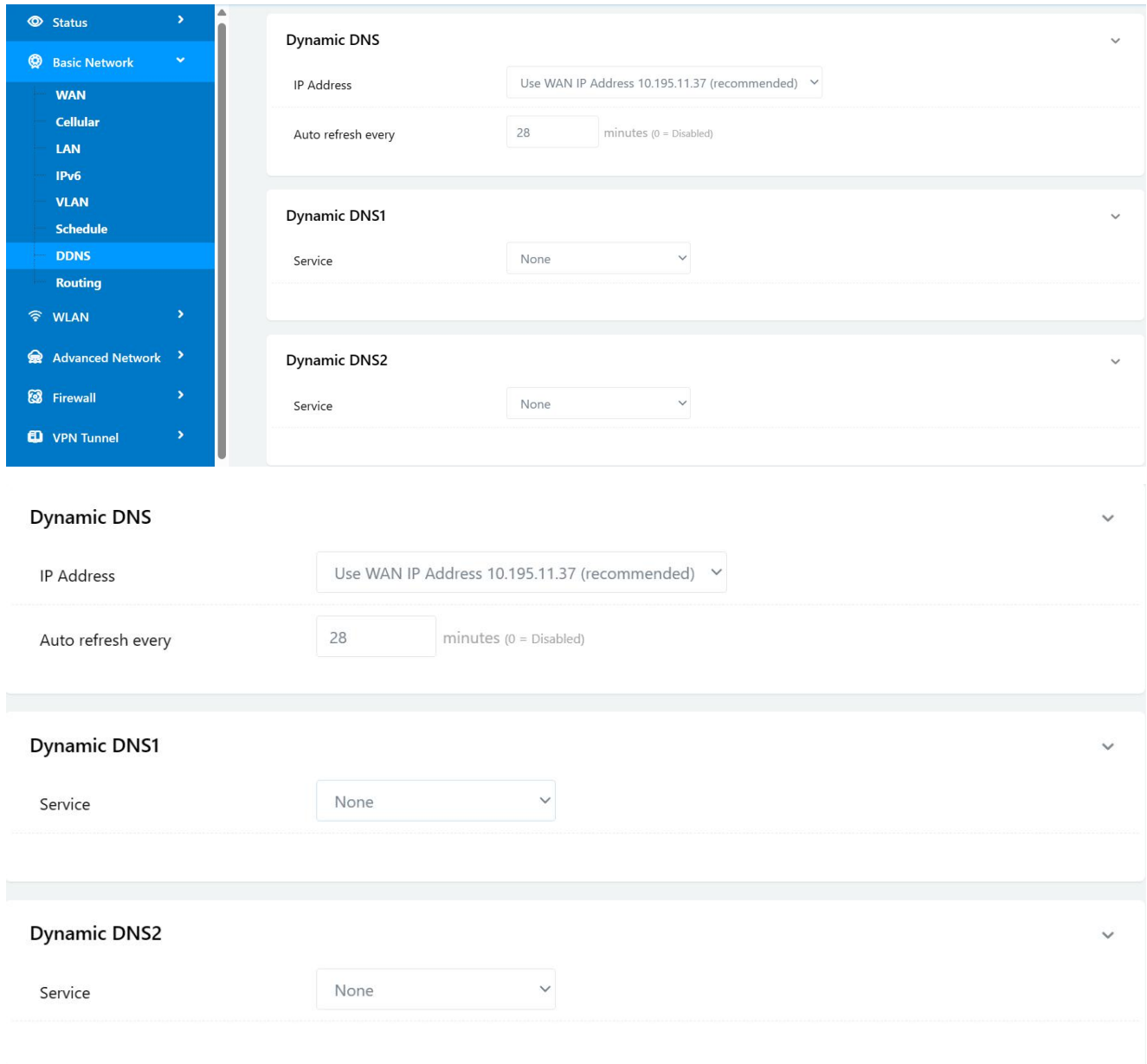


Table 2-5 DDNS Setting Instruction

Parameter	Instruction	Default
IP address	Default is standard DDNS protocol, for customized protocol, please contact Wlink engineer. Usually, use default IP 0.0.0.0	
Auto refresh time	Set the interval of the DDNS client obtains new IP, suggest 240s or above	
Service provider	Select the DDNS service provider that listed.	

Step 2 Please Click “Save” to finish.

----End

2.7.8 Routing Setting

Step 1 Basic Network->Routing to enter the DDNS setting GUI.

- Status >
- Basic Network >
- WAN
- Cellular
- LAN
- IPv6
- VLAN
- Schedule
- DDNS
- Routing
- WLAN >
- Advanced Network >
- Firewall >
- VPN Tunnel >
- Administration >
- More Info

You haven't changed the default password for this router. To change router password [click here](#).

Current Routing Table

Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
default	10.195.11.218	0.0.0.0	0	modem
10.0.0.0	*	255.0.0.0	0	modem
10.195.11.218	*	255.255.255.255	0	modem
127.0.0.0	*	255.0.0.0	0	lo
192.168.1.0	*	255.255.255.0	0	lan

IPv4 Static Routing Table

Destination	Gateway	Subnet Mask	Metric	Interface	Description
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="lan"/>	<input type="text"/>

Add +

Current Routing Table

Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
default	10.195.11.218	0.0.0.0	0	modem
10.0.0.0	*	255.0.0.0	0	modem
10.195.11.218	*	255.255.255.255	0	modem
127.0.0.0	*	255.0.0.0	0	lo
192.168.1.0	*	255.255.255.0	0	lan

IPv4 Static Routing Table

Destination	Gateway	Subnet Mask	Metric	Interface	Description
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="lan"/>	<input type="text"/>

Add +

IPv6 Static Routing Table ▼

Destination	Gateway	Subnet Mask	Metric	Interface	Description
<input type="text"/>	<input type="text"/>	64	0	lan ▼	<input type="text"/>
<input type="button" value="Add +"/>					

Policy Routing Table ▼

Lan	modem	wan	sta	sta2
vlan1 ▼	Auto ▼	Auto ▼	Auto ▼	Auto ▼
<input type="button" value="Add +"/>				

OSPF ▼

Enable OSPF

RFC1583

Router ID

On	Network Address	Area
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Add +"/>		

BGP ▼

Enable BGP

Custom Configuration

BGP Instance ▼

On	AS	Router ID	Description
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Add +"/>			

BGP Network ▼

On	AS	Network	Description
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Add +"/>			

BGP Redistribute ▼

On	AS	Redistribute	Description
<input checked="" type="checkbox"/>	<input style="width: 90%;" type="text"/>	Connected ▼	<input style="width: 90%;" type="text"/>
<input type="button" value="Add +"/>			

BGP Peer ▼

On	AS	Peer	Remote AS	Description
<input checked="" type="checkbox"/>	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>
<input type="button" value="Add +"/>				

BGP Custom Configuration ▼

On	AS	Custom Configuration	Description
<input checked="" type="checkbox"/>	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>
<input type="button" value="Add +"/>			

Miscellaneous ▼

Mode	Gateway ▼
RIPv1 & v2	Disabled ▼
DHCP Routes	<input checked="" type="checkbox"/>
Spanning-Tree Protocol	<input type="checkbox"/>

Table 2-6 Routing Setting Instruction

Parameter	Instruction	Default
Destination	Router can reach the destination IP address.	
Gateway	Next hop IP address which the router will reach	
Subnet Mask	Subnet mask for destination IP address	
Metric	Metrics are used to determine whether one particular route should be chosen over another.	
Interface	Interface from router to gateway.	
Description	Describe this routing name.	

Step 2 Please Click "Save" to finish.

----End

2.8 WLAN Setting

It's mainly for router which support Wi-Fi, you can modify and configure WLAN parameter through Web GUI, below is the common setting.



- WL-R100 doesn't support Wi-Fi feature.
- WL-R130 Wi-Fi feature is optional.
- WL-R200 Wi-Fi feature is optional.
- WL-R210/R230/WL-R520 supports Wi-Fi feature as default.

2.8.1 Basic Setting

Step 1 WLAN->Basic Setting to configure relative parameter

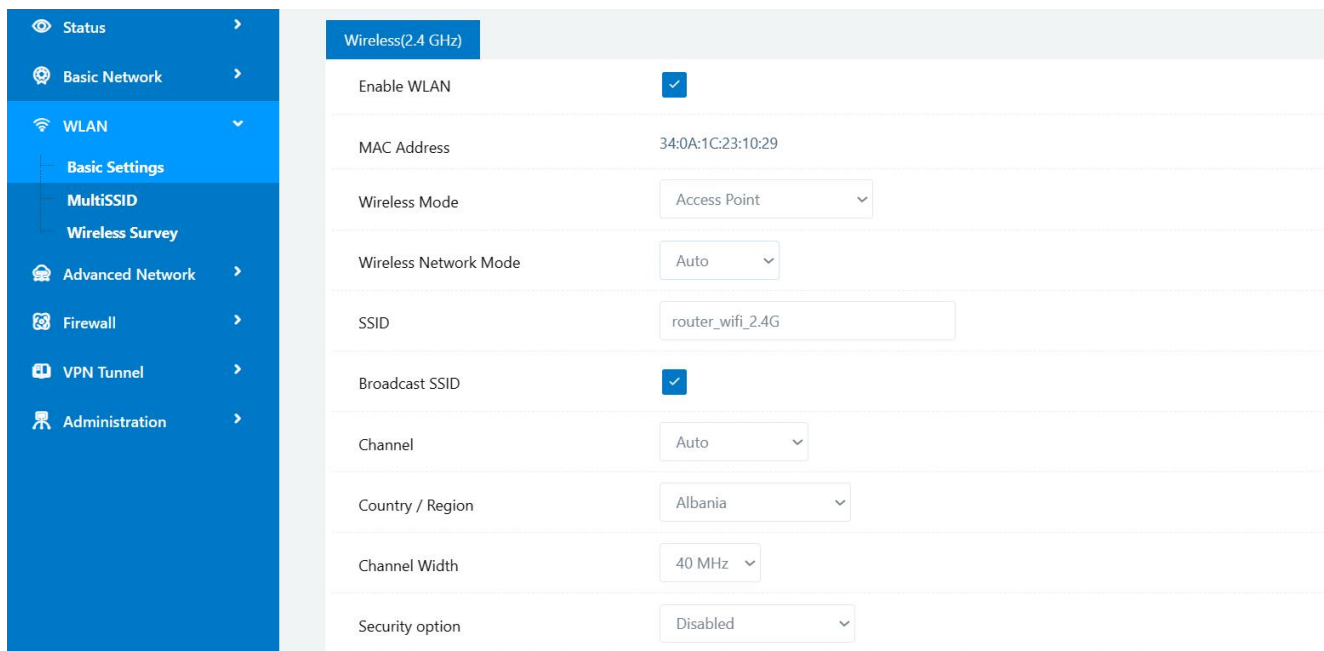


Table 2-7 Basic of WLAN Setting Instruction

Parameter	Instruction	Default
Radio Mode	2.4G model, Wi-Fi bandwidth for 1300Mbps	
Enable wireless	Enable or Disable the Wireless	Enable
Wireless mode	Support AP mode.	Access Point
Wireless Network protocol	Support Auto/b/g/n optional for 2.4G. Support Auto/A/N optional for 2.5G.	
SSID	The default is router, can be modified as per application.	

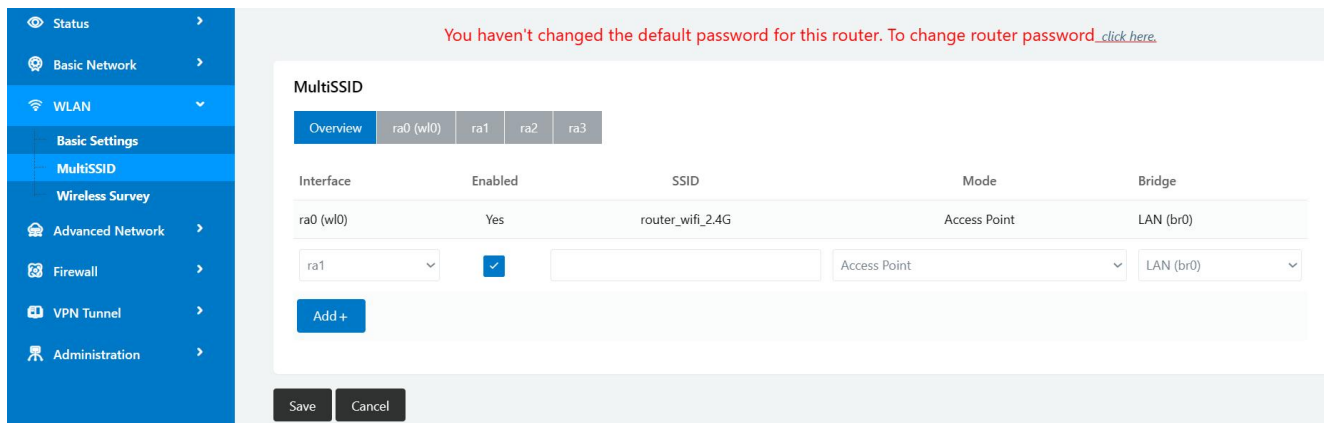
Parameter	Instruction	Default
Channel	The channel of wireless network, suggest keep the default	
Channel Width	20MHz and 40MHz alternative for 2.4G. 20MHz, 40MHz and 80MHz alternative for 2.4G.	
Security	Support various encryption method as requested.	Disabled

Step 2 Please click “Save” to finish.

----End

2.8.2 MultiSSID

Step 1 WLAN> MultiSSID.



Step 2 Please Click “Save” to finish.



NOTE

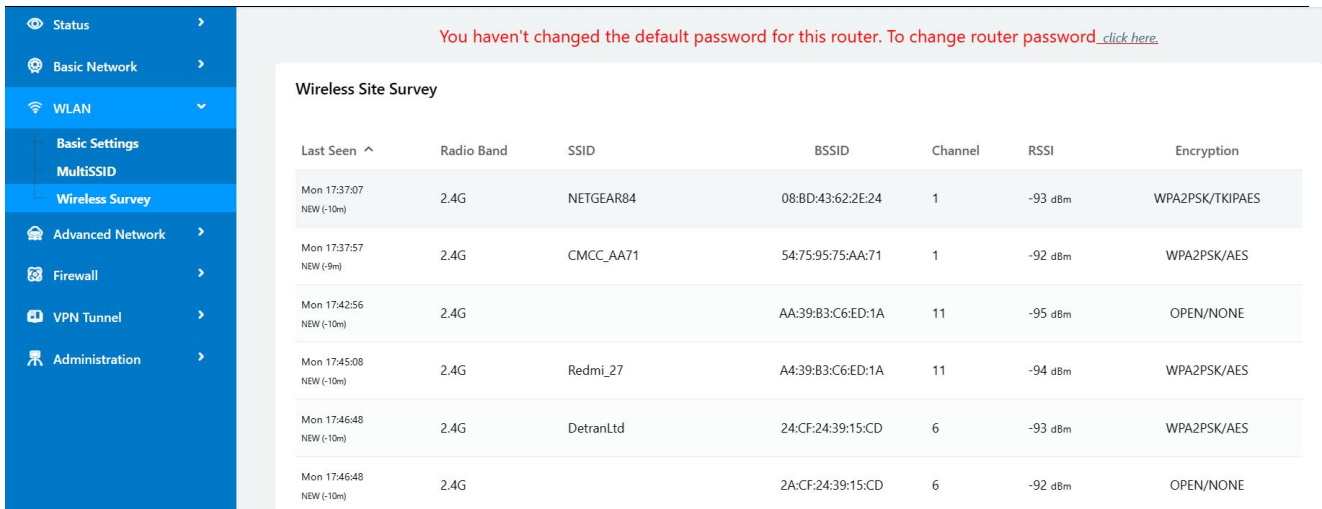
Support 4 SSIDs as Max

----End

2.8.3 Wireless Survey

Step 1 WLAN> Wireless Survey to check survey.

The Router will automatically scan neighbors SSIDs.



Step 2 Please Click "Stop" to change refresh by manual.

---End

2.9 Advanced Network Setting

2.9.1 Port Forwarding

Step 1 Advanced Network > Port Forwarding to enter the GUI, you may modify the router name, Host name and Domain name according to the application requirement.

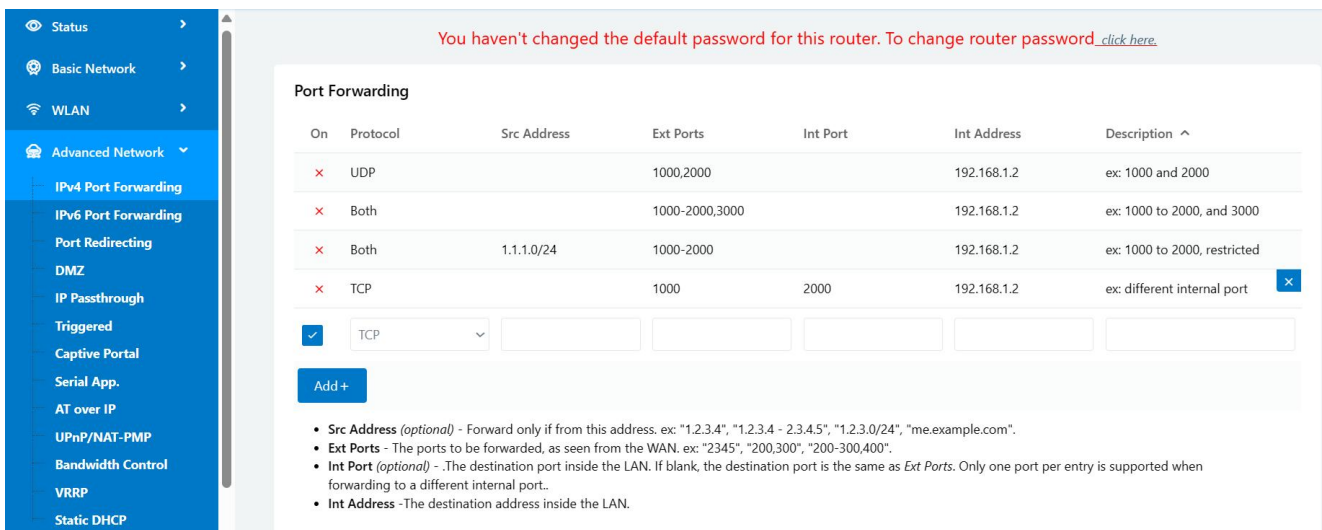


Table 2-8 Port Forwarding Instruction

Parameter	Instruction	Default
Protocol	Support UDP, TCP, both UDP and TCP	
Src. Address	Source IP address. Forward only if from this address.	
Ext. Ports	External ports. The ports to be forwarded, as seen from the WAN.	
Int. Port	Internal port. The destination port inside the LAN. If blank, the	

Parameter	Instruction	Default
	destination port is the same as Ext Ports. Only one port per entry is supported when forwarding to a different internal port.	
Int. Address	Internal Address. The destination address inside the LAN.	
Description	Remark the rule	

Step 2 Please click “save” to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

2.9.2 Port Redirecting

Step 1 Advanced Network > Port Redirecting to enter the GUI, you may modify the router name, Host name and Domain name according to the application requirement.

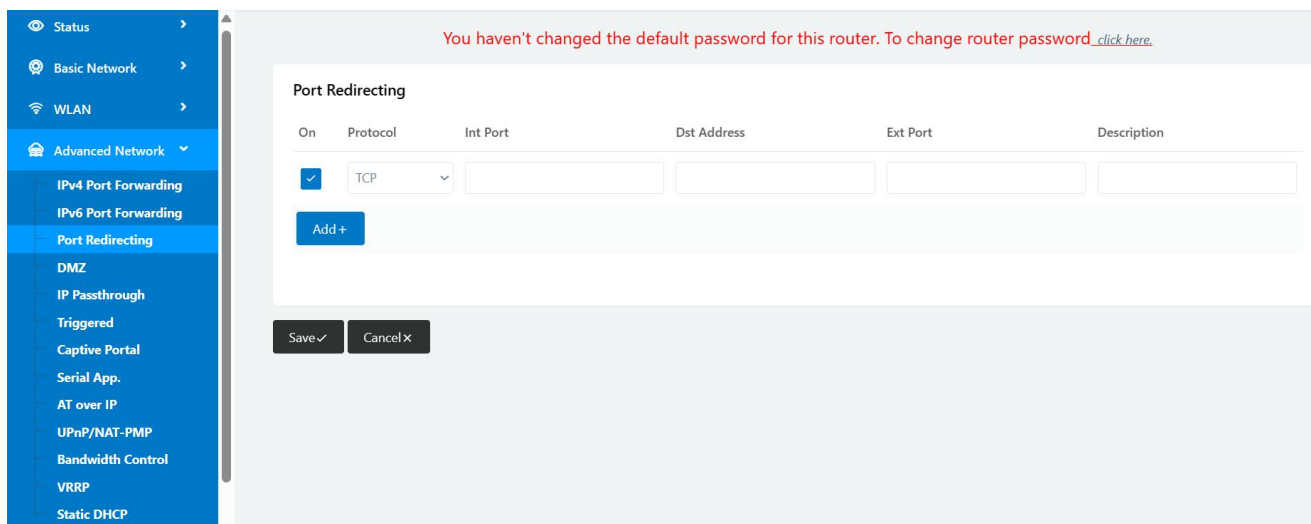


Table 2-9 Port Redirecting Instruction

Parameter	Instruction	Default
Protocol	Support UDP, TCP, both UDP and TCP	
Int Port	Internal port.	
Dst Address	The redirecting IP address.	
Ext Ports	External port for redirection.	
Description	Remark the rule	

Step 2 Please click “save” to finish.



NOTE

The Port redirecting feature will be unavailable when enable Captive Portal function.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

2.9.3 DMZ Setting

Step 1 Advanced Network> DMZ to check or modify the relevant parameter.

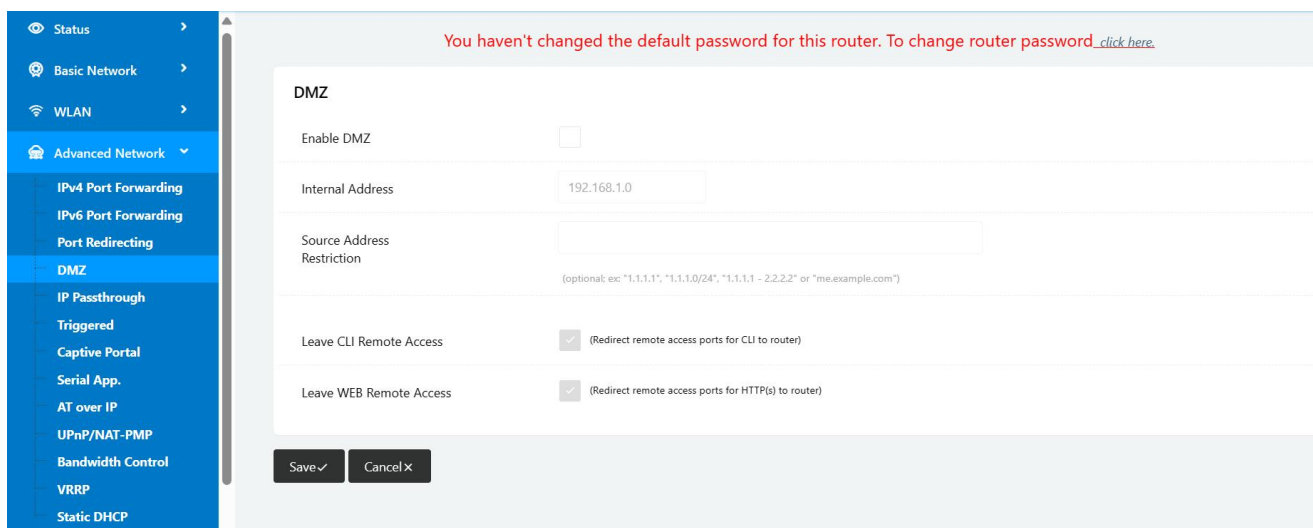


Table 2-10 DMZ Instruction

Parameter	Instruction	Default
Destination Address	The destination address inside the LAN.	
Source Address Restriction	If no IP address inside, it will allow all IP address to access. If define IP address, it will just allow the defined IP address to access.	
Leave Remote Access		

Step 2 Please click “save” to finish

----End

2.9.4 IP Passthrough Setting

Step 1 Advanced Network> IP Passthrough to check or modify the relevant parameter.

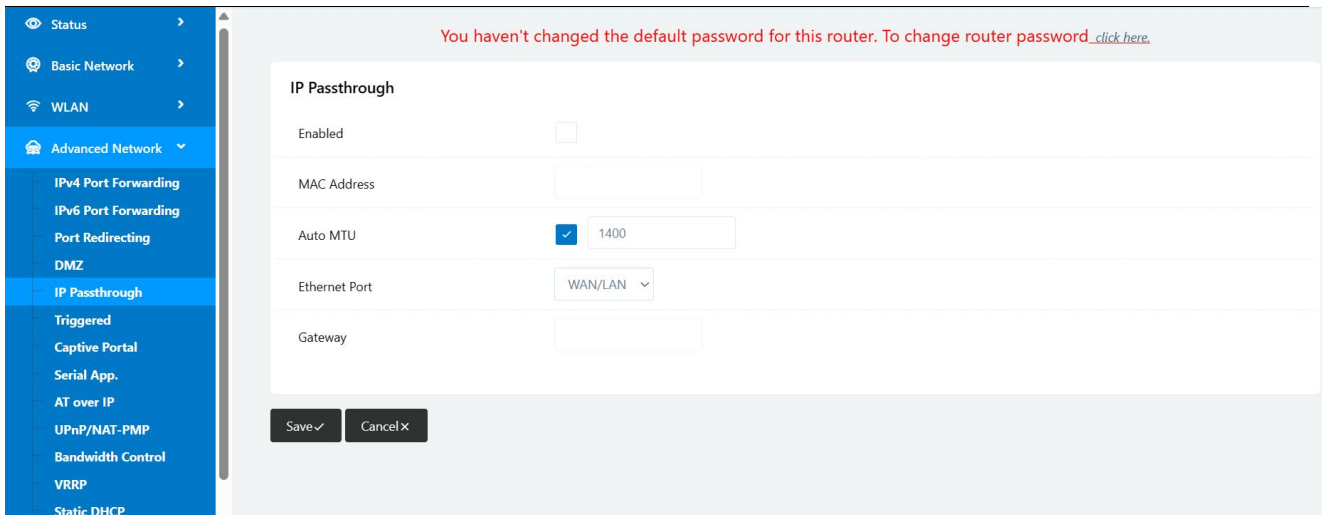


Table 2-11 IP Passthrough Instruction

Parameter	Instruction	Default
Enable	Enable IP Passthrough	Disabled
MAC Address	Enable DHCP of device. Configure device Mac. Device will be assigned SIM IP.	
Gateway	If WL-Rxx router connect to multiple device, input other device gateway. The device might access to router GUI.	

Step 2 Please click “save” to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

2.9.5 Triggered Setting

Step 1 Advanced Network> Triggered to check or modify the relevant parameter.

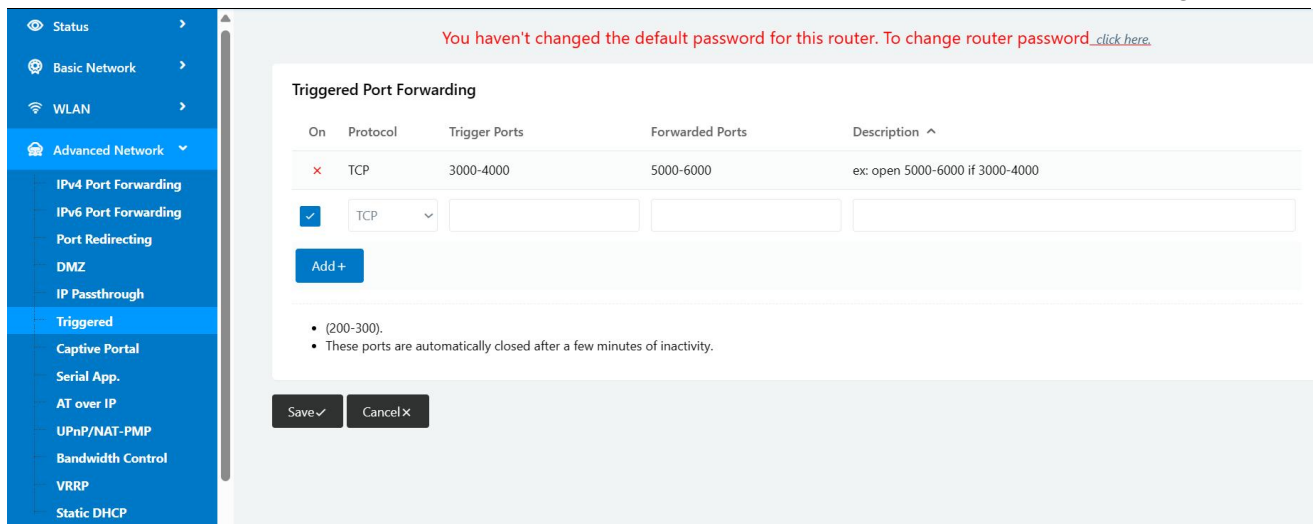


Table 2-12 Triggered Instruction

parameter	Instruction	Default
Protocol	Support UDP, TCP, both UDP and TCP	
Triggered Ports	Trigger Ports are the initial LAN to WAN "trigger".	
Transferred Ports	Forwarded Ports are the WAN to LAN ports that are opened if the "trigger" is activated.	
Note	Port triggering opens an incoming port when your computer is using a specified outgoing port for specific traffic.	

Step 2 Please click “save” to finish.

----End

2.9.6 Captive Portal

Step 1 Advanced Network> Triggered to check or modify the relevant parameter.

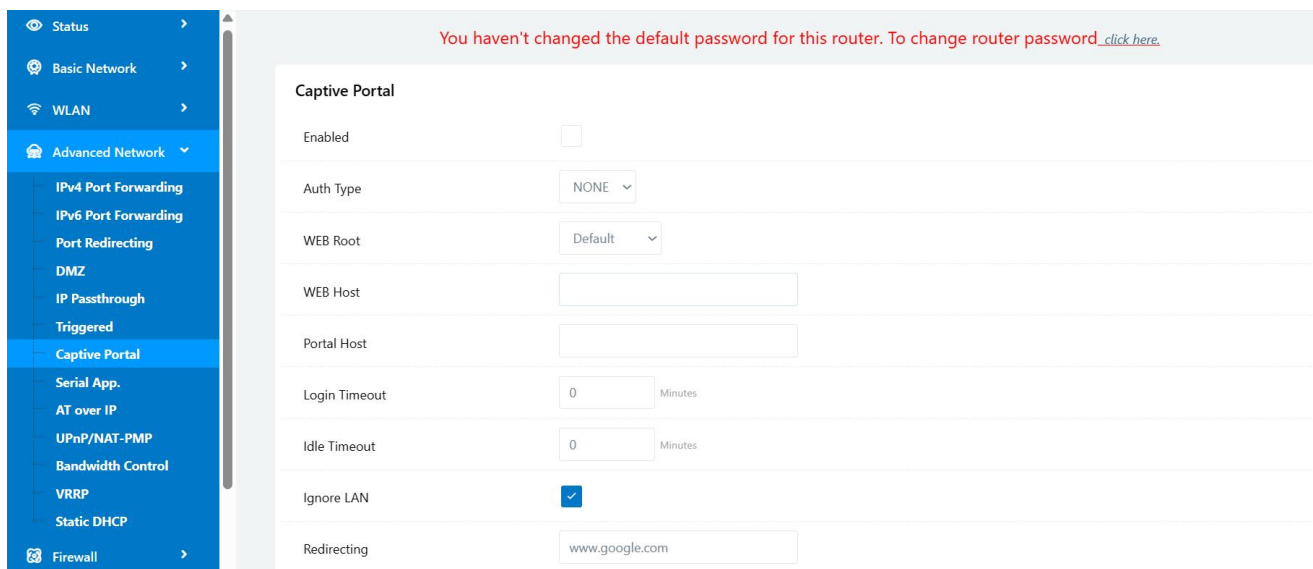


Table 2-13 Captive Portal Instruction

Parameter	Instruction	Default
Enable	Enable Captive portal feature.	
Auth Type	Reserved.	
Web Root	Choose captive portal file storage path. Default: Captive portal file is in the firmware as default. In-storage: Captive portal file is in router's Flash. Ex-storage: Captive portal file is in extended storage such as SD card.	
Web Host	Configure domain name for the captive portal access. For example, Configure as wlink.tech.com, we might directly access to captive portal page in the website as wlink.tech.com	
Portal Host	Reserved.	
Logged Timeout	Maximum time user has connectivity. User need to re-login Captive Portal page after defined time.	
Idle Timeout	Maximum time user has connectivity if no network activity from Wi-Fi User.If User need to re-login Captive page to surf internet.	
Ignore LAN	If enabled, LAN devices will bypass the Captive Portal page.	
Redirecting	Router will redirect to the defined link after accepting the terms and conditions on the Captive Portal page.	
MAC Whitelist	No captive portal page for Wi-Fi device.	
Download QoS	Enable to apply the Download and Upload per user limits.	
Upload Qos	Maximum download speed available to each user.	

Step 2 Please click “save” to finish.



WL-R100 doesn't support Captive Portal feature.



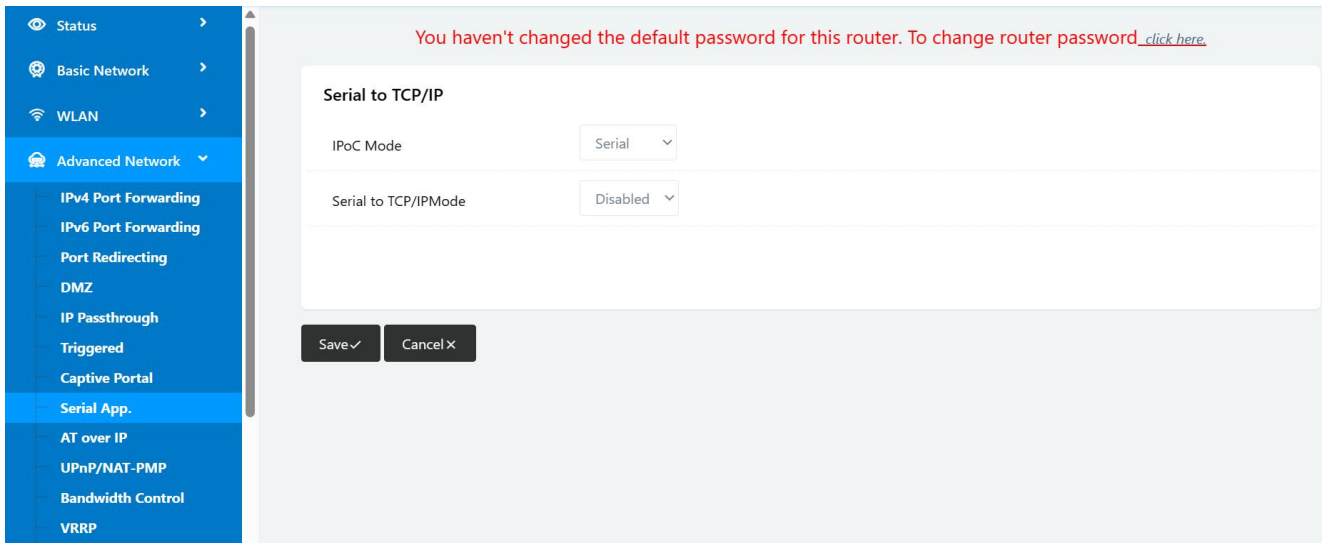
Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

2.9.7 Serial App.

Step 1 Advanced Network> Serial App to check or modify the relevant parameter.



Serial to TCP/IP	
IPoC Mode	Serial
Serial to TCP/IP Mode	Client
Server IP/Port	8.8.8.8 : 40002
Socket Type	TCP
Socket Timeout	500 (milliseconds)
Serial Timeout	500 (milliseconds)
Packet Payload	1024 (bytes)
Heart-Beat Content	
Heart-Beat Interval	2 (seconds)
Port Type	RS485/RS232

Cache Enable	<input checked="" type="checkbox"/>
Debug Enable	<input type="checkbox"/>
Baud Rate	57600 ▼
Parity Bit	none ▼
Data Bit	8 ▼
Stop Bit	1 ▼

Table 2-14 Serial App Instruction

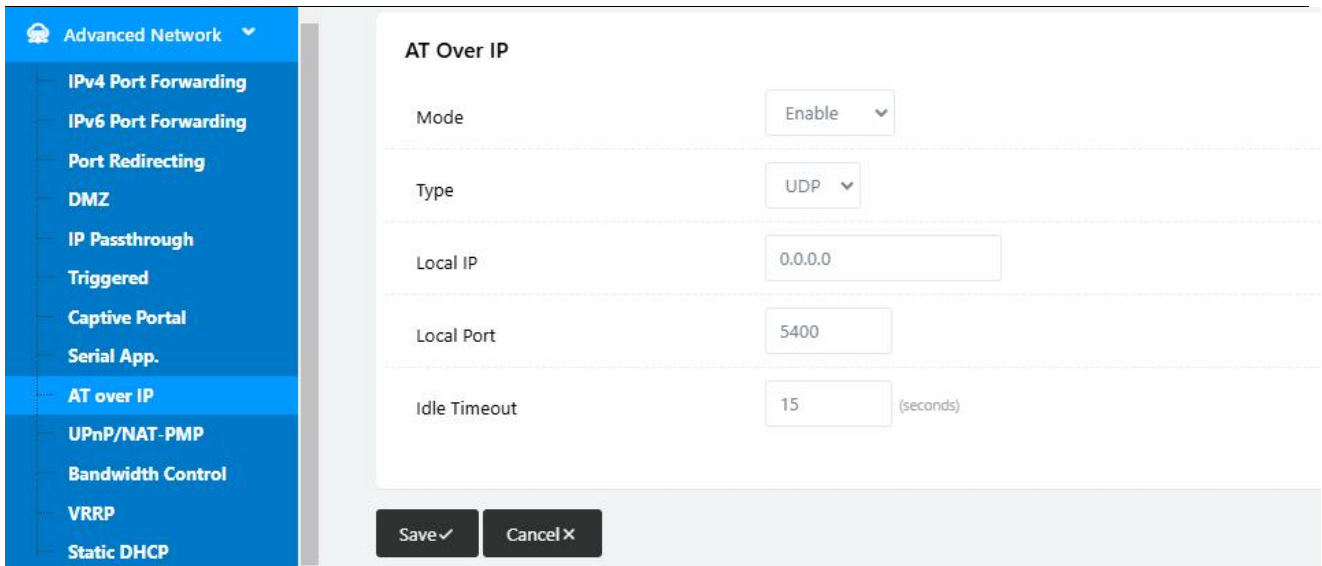
Parameter	Instruction	Default
Serial to TC/IP mode	Support Disable, Server and Client mode. Such as Client.	
Server IP/Port	IP address and domain name are acceptable for Server IP	
Socket Type	Support TCP/UDP protocol	
Socket Timeout	Router will wait the setting time to transmit data to serial port.	
Serial Timeout	Serial Timeout is the waiting time for transmitting the data package that is less the Packet payload. If the last package equals to the Packet payload, Serial port will transmit it immediately. The default setting is 500ms.	
Packet payload	Packet payload is the maximum transmission length for serial port data packet. The default setting is 1024bytes.	
Heart-beat Content	Send heartbeat to the defined server to keep router online. Meantime, it's convenient to monitor router from server.	
Heartbeat Interval	Heartbeat interval time	
Baud Rate	115200 as default	115200
Parity Bit	None as default	
Data Bit	8bit as default	8bit
Stop Bit	1bit as default	1bit

Step 2 Please click "save" to finish.

----End

2.9.8 AT Over IP

Step 1 Advanced Network> AT Over IP to check or modify the relevant parameter.



Step 2 Please click “save” to finish.



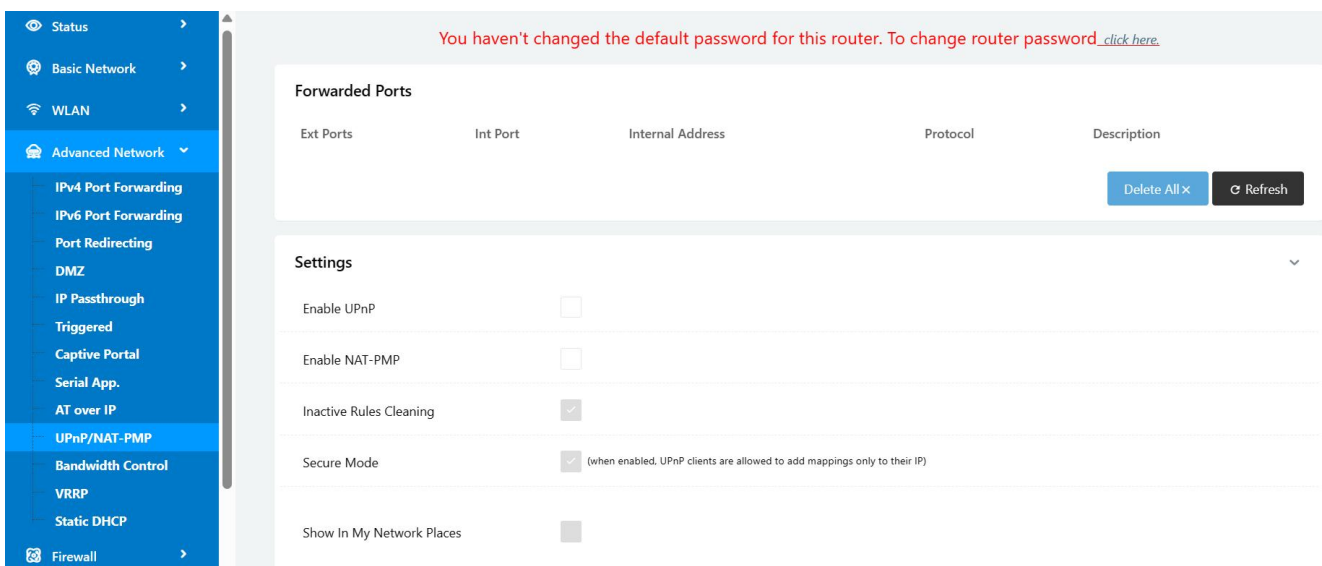
Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

2.9.9 UPnp/NAT-PMP Setting

Step 3 Advanced Network> Upnp/NAT-PMP to check or modify the relevant parameter.



Step 4 Please click “save” to finish.

----End

2.9.10 Bandwidth Control Setting

Step 1 Advanced Network> Bandwidth Control to check or modify the relevant parameter.

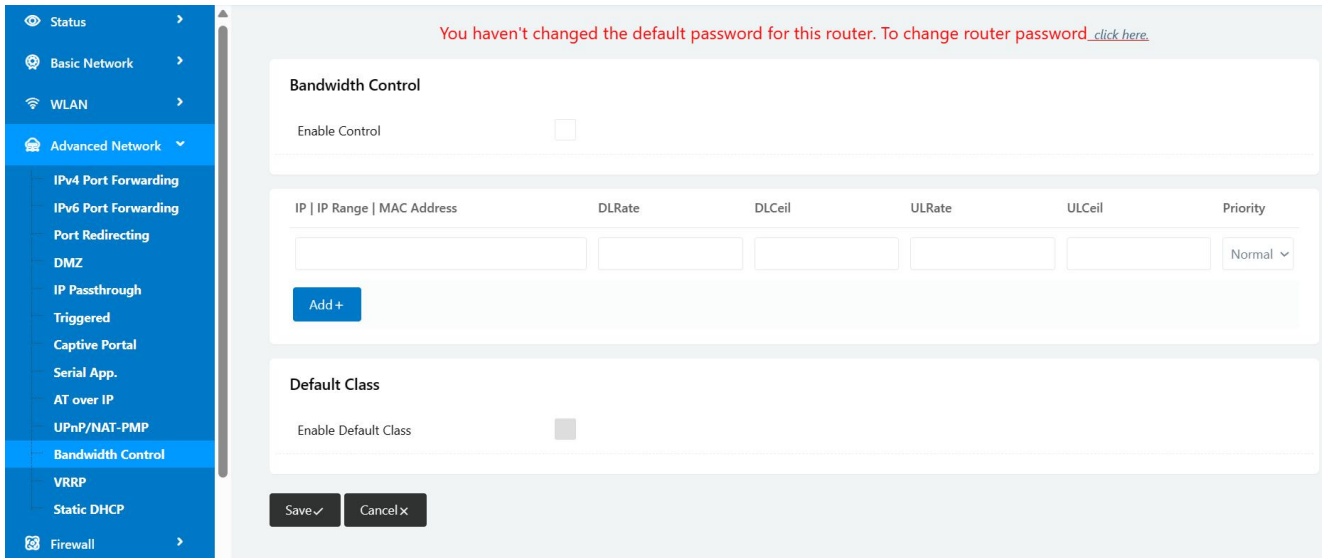


Table 2-15 Bandwidth Control Instruction

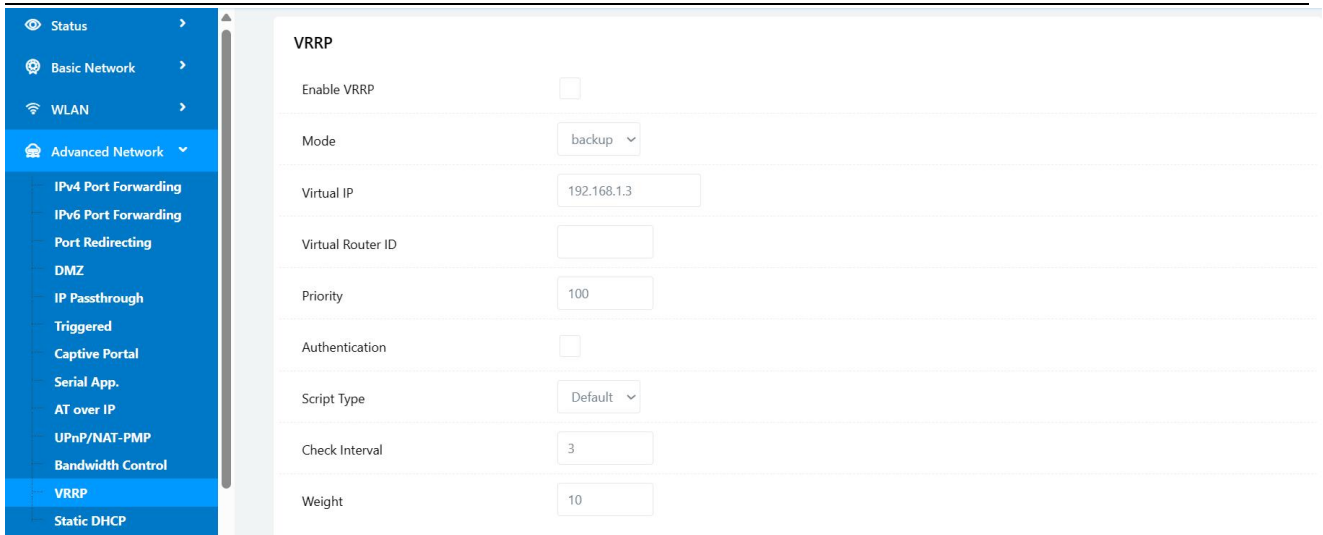
Parameter	Instruction	Default
Max Available Download	Speed limit for router.	
Max Available Upload	Speed limit for router.	
IP/ IP Range/ MAC Address	Limit devices speed for specified IP/IP Range/ MAC Address.	
DL Rate	Mix Download rate	
DL ceil	Max download rate	
UL Rate	Mix Upload rate	
UL ceil	Max upload rate	
Priority	The priority of a specific user.	
Default Class	If no specified IP/MAC, the download and upload limit for total speed for all of device.	

Step 2 Please click “save” to finish.

----End

2.9.11 VRRP Setting

Step 1 Advanced Network> VRRP to check or modify the relevant parameter.

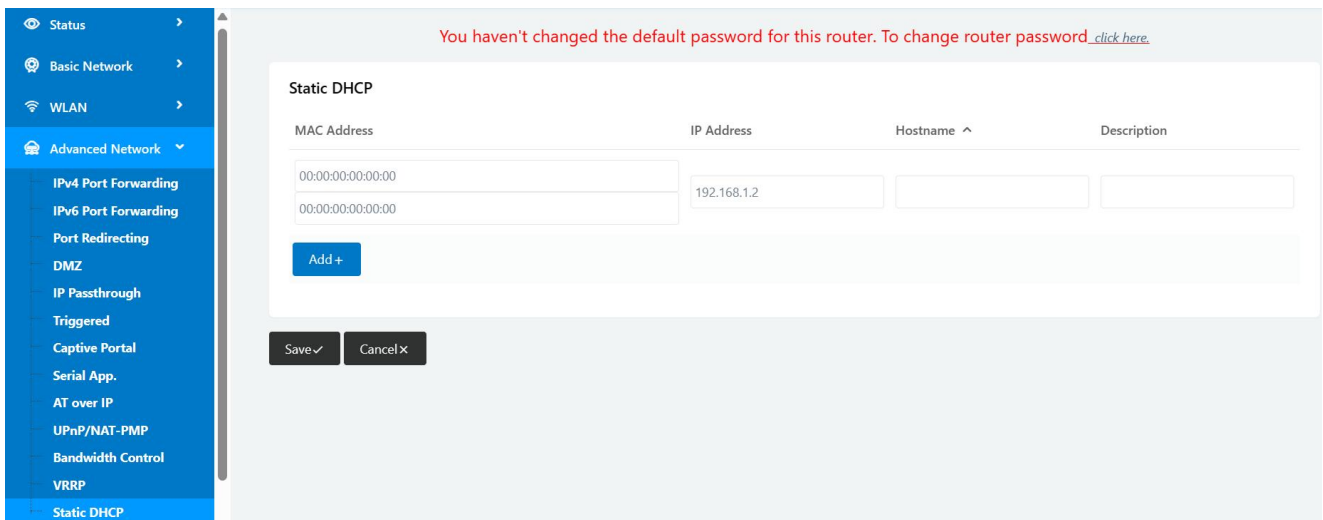


Step 2 Please click “save” to finish.

----End

2.9.12 Static DHCP Setting

Step 1 Advanced Network> Static DHCP to check or modify the relevant parameter.



Step 2 Please click “save” to finish.

----End

2.10 Firewall

2.10.1 IP/URL Filtering

Step 1 Firewall> IP/URL Filtering to check or modify the relevant parameter.

IP/MAC/Port Filtering

On	Network Protocol	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>	IPv4				NONE			Accept	

Key Word Filtering

On	Key Word	Description
<input checked="" type="checkbox"/>		

URL Filtering

On	URL	Description
<input checked="" type="checkbox"/>		

Access Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>				NONE			Accept	

Table 2-16 IP/URL Filtering Instruction

Parameter	Instruction	Default
IP/MAC/Port Filtering	Support IP address, MAC address and port filter. Accept/Drop options for filter policy.	

Parameter	Instruction	Default
Key Word Filtering	Support key word filter.	
URL Filtering	Support URL filter.	
Access Filtering	Support Access Filter.	



Please check Firewall rule in Configuration instance.

Step 2 Please click “save” to finish.

---End

2.10.2 Domain Filtering

Step 1 Firewall> Domain Filtering to check or modify the relevant parameter.

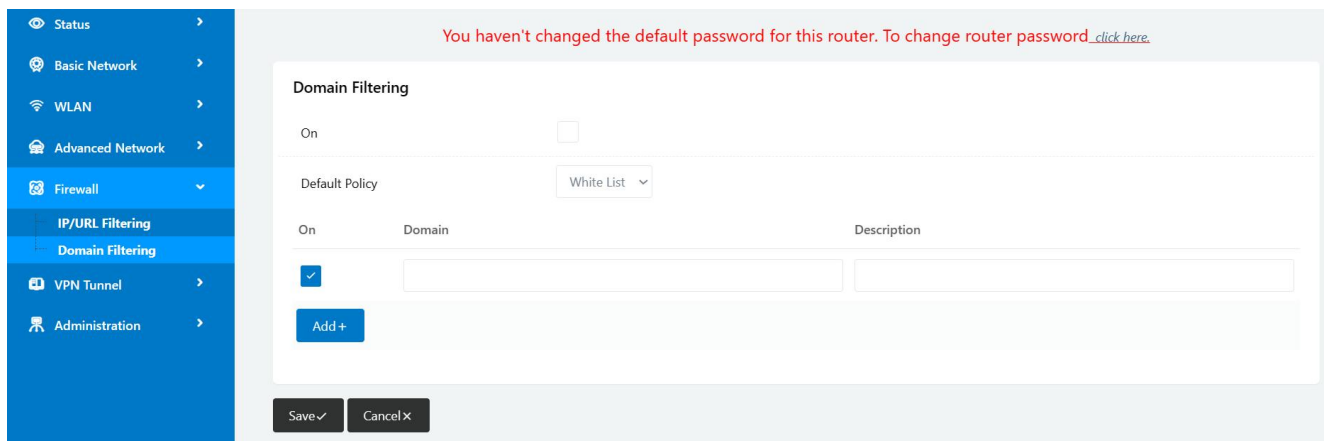


Table 2-17 Domain Filtering Instruction

Parameter	Instruction	Default
Default Policy	Support black list and white list	
Local IP Address	Local IP address for LAN.	
Domain	Support Domain filter.	

Step 2 Please click “save” to finish.

----End

2.11 VPN Tunnel

2.11.1 Wireguard Setting

Step 1 VPN Tunnel> Wireguard to check or modify the relevant parameter.

The screenshot displays the 'Wireguard' configuration page. On the left is a navigation menu with options like Status, Basic Network, Advanced Network, Firewall, VPN Tunnel (selected), GRE, OpenVPN Client, OpenVPN Server, PPTP/L2TP Server, PPTP/L2TP Client, L2TP V3, IPsec, DMVPN, and Administration. The main area contains the following settings:

- Enabled:** A checked checkbox.
- Mode:** A dropdown menu set to 'Client'.
- Peer IP/Port:** Input fields for '192.168.1.2' and ': 51821'.
- Local Key:** An input field containing 'test'.
- Local IP/Mask:** Input fields for '192.168.88.1/24' and an example 'ex. 192.168.88.5/24'.
- Peer Key:** An input field containing 'test'.
- Preshared Key:** An empty input field.
- Persistent Keepalive:** An input field containing '25'.
- Allowed IPS:** An input field containing '0.0.0.0/0' and an example 'ex. 192.168.88.0/24 or 192.168.88.0/24,192.168.99.0/24'.
- Peer Subnet IP/Mask:** An empty input field and an example 'ex. 192.168.88.0/24 or 192.168.88.0/24,192.168.99.0/24'.

At the bottom of the configuration area are 'Save ✓' and 'Cancel ✕' buttons.

Table 2-18 Wireguard Client Instruction

Parameter	Instruction	Default
Enable	Eenable Wireguard.	
Model	Wireguard client and server modes optional	
Peer IP/Port	Server IP and port	
Local Key	VPN local key	
Local IP/Mask	Wireguard VPN tunnel local IP and mask. The VPN local IP address and peer IP address are different subnet segment.	
Peer Key	VPN peer key	
Preshared Key	Wireguard Pre-shared key	
Keepalive	Keepalive interval,unit for second	
Allowed IPs	Allowed VPN subnet IP addresses	
Peer Subnet IP/Mask	Wireguard VPN tunnel Peer IP and mask.	

Wireguard

Enabled

Mode

Bind Port

Local Key

Local IP/Mask ex. 192.168.88.5/24

Peer Subnet IP/Mask ex. 192.168.88.0/24 or 192.168.88.0/24,192.168.99.0/24

Allowed IPS Persistent Keepalive Peer Key

Table 2-19 Wireguard Sever Instruction

Parameter	Instruction	Default
Enable	Eenable Wireguard.	
Model	Wireguard client and server modes optional	
Bind Port	Wireguard server port	
Local Key	VPN local key	
Local IP/Mask	Wireguard VPN tunnel local IP and mask. The VPN server local IP address and client IP address are different subnet segments.	
Preshared Key	Wireguard Pre-shared key	
Keepalive	Keepalive interval,unit for second	
Allowed IPs	Allowed VPN subnet IP addresses	
Peer Key	VPN peer key	

Step 2 Please click "save" to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

2.11.2 Zerotier Setting

Step 1 VPN Tunnel> Zerotier to check or modify the relevant parameter.

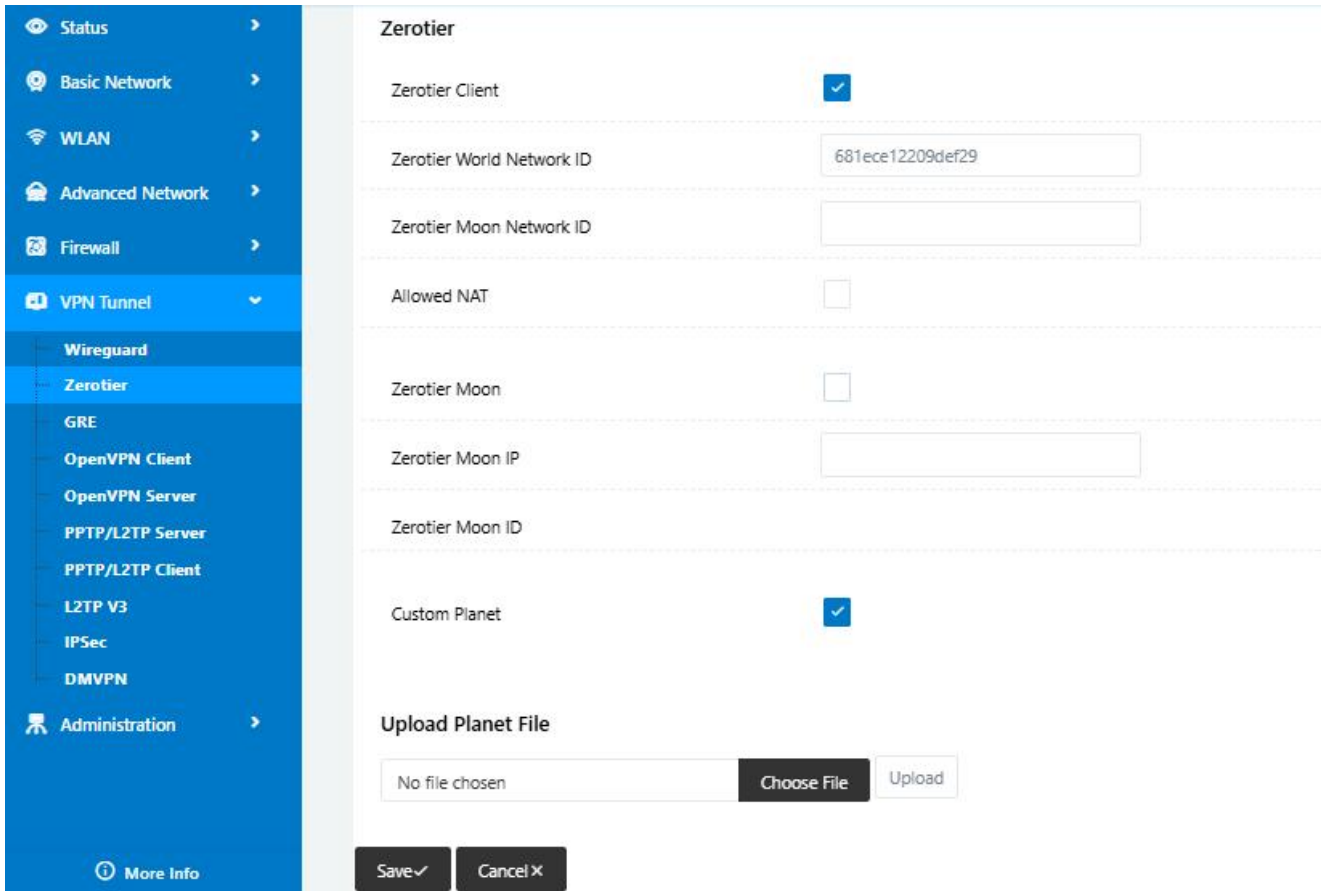


Table 2-20 Zerotier Instruction

Parameter	Instruction	Default
Enable	Enable Zerotier Client mode	Disable
Zerotier World Network ID	A unique 16-digit identifier for your ZeroTier network. Nodes must join using this ID.	Null
Zerotier Moon Network ID	ZeroTier Moon server Network ID	Null
Allowed NAT	Enable NAT in zerotier network.It function will be configured with zerotier IP management together to allow the defined zerotier client access.	Disable
Zerotier Moon	Private Root Servers as Moon server	Disable
Zerotier Moon IP	Moon server IP address	Null
Zerotier Moon ID	A unique 16-digit identifier for private ZeroTier network.	Null
Custom Planet	Custom Planet configuration	Disable
Allowed IPs	Allow access to other Zerotier clients. IP is the LAN segment address of other ZeroTier clients; The gateway is a VPN address of other ZeroTier clients.The IP and gateway must correspond to the same routing.	Null

Parameter	Instruction	Default
Upload Planet File	Upload the updated Planet file	Null

Step 2 Please click “save” to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

2.11.3 GRE Setting

Step 1 VPN Tunnel> GRE to check or modify the relevant parameter.

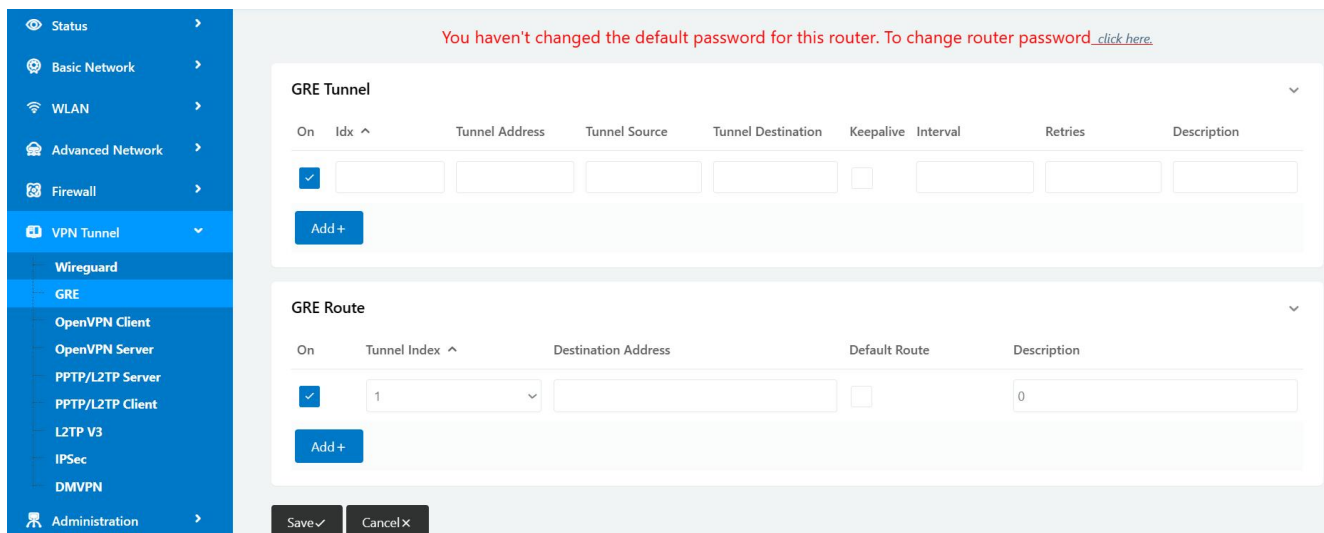


Table 2-21 GRE Instruction

Parameter	Instruction	Default
Idx	GRE tunnel number	
Tunnel Address	GRE Tunnel local IP address which is a virtual IP address.	
Tunnel Source	Router's 3G/WAN IP address.	
Tunnel Destination	GRE Remote IP address. Usually a public IP address	
Keep alive	GRE tunnels keep alive to keep GRE tunnel connection.	
Interval	Keep alive interval time.	
Retries	Keep alive retry times. After retrying times, GRE tunnel will be re-established.	
Description		

Step 2 Please click “save” to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

2.11.4 OpenVPN Client Setting

Step 1 VPN Tunnel> OpenVPN Client to check or modify the relevant parameter.

The screenshot displays the 'OpenVPN Client' configuration page. At the top, a red warning message states: "You haven't changed the default password for this router. To change router password [click here](#)." Below this, the 'OpenVPN Client' section is visible, with tabs for 'Client 1' and 'Client 2'. Underneath, there are sub-tabs for 'Basic', 'Advanced', 'Keys', and 'Status'. The 'Basic' tab is active, showing the configuration for 'VPN Client #1 (Stopped)'. The settings are as follows:

- Start with WAN:
- Interface Type: TUN (dropdown)
- Protocol: UDP (dropdown)
- Server Address: [] 1194
- Firewall: Automatic (dropdown)
- Authorization Mode: TLS (dropdown)

OpenVPN Client

Client 1

Client 2

Basic

Advanced

Keys

Status

VPN Client #1 (Stopped)

Start with WAN

Interface Type TUN ▼

Protocol UDP ▼

Server Address

Firewall Automatic ▼

Authorization Mode TLS ▼

Username/Password Authentication

HMAC authorization Disabled ▼

Create NAT on tunnel

Table 2-22 Basic of OpenVPN Instruction

Parameter	Instruction	Default
Start with WAN	Enable the OpenVPN feature for 4G/3G/WAN port.	
Interface Type	Tap and Tun type are optional. Tap is for bridge mode and Tunnel is for routing mode.	
Protocol	UDP and TCP optional.	
Server Address	The OpenVPN server public IP address and port.	
Firewall	Auto, External only and Custom are optional	
Authorization Mode	TLS, Static key and Custom are optional.	
Username/Password Authentication	As the configuration requested.	
HMAC authorization	As the configuration requested.	
Create NAT on tunnel	Configure NAT in OpenVPN tunnel.	

Basic Advanced Keys Status

VPN Client #1 (Stopped)

Poll Interval: (in minutes, 0 to disable)

Redirect Internet traffic:

Accept DNS configuration:

Encryption cipher:

Compression:

TLS Renegotiation Time: (in seconds, -1 for default)

Connection retry: (in seconds; -1 for infinite)

Verify server certificate (tls-remote):

Custom Configuration:

Table 2-23 Advanced of OpenVPN Instruction

Parameter	Instruction	Default
Poll Interval	OpenVPN client check router's status as interval time.	
Redirect Internet Traffic	Configure OpenVPN as default routing.	
Access DNS	As the configuration requested.	
Encryption	As the configuration requested.	
Compression	As the configuration requested.	
TLS Renegotiation Time	TLS negotiation time. -1 as default for 60s.	
Connection Retry Time	OpenVPN retry to connection interval.	
Verify server certificate	As the configuration requested.	
Custom Configuration	As the configuration requested.	

Basic Advanced **Keys** Status

VPN Client #1 (Stopped) ▶

For help generating keys, refer to the OpenVPN HOWTO.

Certificate Authority

Client Certificate

Client Key

Table 2-24 Keys of OpenVPN Instruction

Parameter	Instruction	Default
Certificate Authority	Keep certificate as the same as server	
Client Certificate	Keep client certificate as the same as server	
Client Key	Keep client key as the same as server	

Basic Advanced Keys **Status**

VPN Client #1 (Stopped) ▶

Client is not running or status could not be read.

[Refresh Status](#)

Table 2-25 Status of OpenVPN Instruction

Parameter	Instruction	Default
Status	Check OpenVPN status and data statistics.	

Step 2 Please click “save” to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

2.11.5 OpenVPN Server Setting

Step 1 VPN Tunnel> OpenVPN Server to check or modify the relevant parameter.

The screenshot shows the configuration page for the OpenVPN Server. On the left is a navigation menu with options: Status, Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel (selected), Wireguard, Zerotier, GRE, OpenVPN Client, OpenVPN Server (highlighted), PPTP/L2TP Server, PPTP/L2TP Client, L2TP V3, IPsec, DMVPN, and Administration. Below the menu is a 'More Info' link.

The main content area is titled 'Server 1' and 'Server 2'. It has tabs for 'Basic', 'Advanced', 'Keys', and 'Status'. The 'Basic' tab is active, showing 'VPN Server #1 (Stopped)'. The configuration parameters are as follows:

Parameter	Value
Start with WAN	<input type="checkbox"/>
Interface Type	TUN
Protocol	UDP
Port	1194
Firewall	Automatic
Authorization Mode	TLS
Extra HMAC authorization (tls-auth)	Disabled
VPN subnet/netmask	10.8.0.0 / 255.255.255.0

At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

The screenshot displays the configuration page for VPN Server #1. At the top, there are tabs for 'Server 1' and 'Server 2'. Below that are sub-tabs for 'Basic', 'Advanced', 'Keys', and 'Status'. The main content area is titled 'VPN Server #1 (Stopped)'. It contains several configuration items, each with a label and a control element:

- Start with WAN:** A checkbox that is checked.
- Interface Type:** A dropdown menu set to 'TUN'.
- Protocol:** A dropdown menu set to 'UDP'.
- Port:** A text input field containing '1194'.
- Firewall:** A dropdown menu set to 'Automatic'.
- Authorization Mode:** A dropdown menu set to 'TLS'.
- Extra HMAC authorization (tls-auth):** A dropdown menu set to 'Disabled'.
- VPN subnet/netmask:** Two text input fields containing '10.8.0.0' and '255.255.255.0'.

Table 2-26 Basic of OpenVPN Instruction

Parameter	Instruction	Default
Start with WAN	Enable the OpenVPN feature for 4G/3G/WAN port.	
Interface Type	Tap and Tun type are optional. Tap is for bridge mode and Tunnel is for routing mode.	
Protocol	UDP and TCP optional.	
Server Port	The OpenVPN server public IP address and port.	
Firewall	Auto, External only and Custom are optional	
Authorization Mode	TLS, Static key and Custom are optional.	
Username/Password Authentication	As the configuration requested.	
HMAC authorization	As the configuration requested. Bi-directional, Incoming, Outgoing optional.	Disable
VPN subnet/netmask	OpenVPN server subnet ip address and mask.	NULL

Basic **Advanced** Keys Status

VPN Server #1 (Stopped)

Poll Interval (in minutes, 0 to disable)

Push LAN to clients

Direct clients to redirect Internet traffic

Respond to DNS

Encryption cipher ▾

Compression ▾

TLS Renegotiation Time (in seconds, -1 for default)

Manage Client-Specific Options

Allow User/Pass Auth

Custom Configuration

Table 2-27 Advanced of OpenVPN Instruction

Parameter	Instruction	Default
Poll Interval	OpenVPN client check router's status as interval time.	
Redirect Internet Traffic	Configure OpenVPN as default routing.	
Respond to DNS	Server respond to client DNS	Disable
Encryption	As the configuration requested.	
Compression	As the configuration requested.	
TLS Renegotiation Time	TLS negotiation time. -1 as default for 60s.	
Manage Client-Specific Option	OpenVPN retry to connection interval.	
Allow User/Pass Auth	Configured the username and password for user authentication.	Disable
Custom Configuration	As the configuration requested.	

Basic Advanced **Keys** Status

VPN Server #1 (Stopped)

For help generating keys, refer to the OpenVPN HOWTO.

Static Key

Certificate Authority

Server Certificate

Server Key

Diffie Hellman parameters

Table 2-28 Keys of OpenVPN Instruction

Parameter	Instruction	Default
Static Key	OpenVPN server	NULL
Certificate Authority	Configure Certificate Authority	NULL
Server Certificate	Configure server certificate	NULL
Server Key	Configure server key	NULL
Diffie Hellman parameters	Configure server HD	NULL

Basic Advanced **Keys** Status

VPN Client #1 (Stopped)

Client is not running or status could not be read.

Refresh Status

Start Now

Table 2-29 Status of OpenVPN Instruction

Parameter	Instruction	Default
Status	Check OpenVPN status and data statistics.	

Step 2 Please click “save” to finish.

Please check lock bank configuration in the chapter 3 as reference.

---End

2.11.6 PPTP/L2TP Sever Setting

Step 1 VPN Tunnel> PPTP/L2TP Sever to check or modify the relevant parameter.

The screenshot displays the configuration interface for the PPTP/L2TP Server. On the left is a navigation menu with options like Status, Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel, Wireguard, Zerotier, GRE, OpenVPN Client, OpenVPN Server, PPTP/L2TP Server (selected), PPTP/L2TP Client, L2TP V3, IPSec, DMVPN, and Administration. The main area shows the following settings:

- Enable:** Checked (blue box).
- Local IP Address/Netmask:** 192.168.1.1 / 255.255.255.0
- Remote IP Address Range:** 172.19.0.1 - 172.19.0.6 (6)
- Broadcast Relay Mode:** Disabled (with a red warning: "Enabling this may cause HIGH CPU usage")
- Protocol Type:** PPTP
- Encryption:** MPPE-128
- DNS Servers:** 0.0.0.0
- WINS Servers:** 0.0.0.0
- MTU:** 1450

Table 2-30 PPTP/L2TP Server Basic Instruction

parameter	Instruction	Default
Enable	VPN enable	Disable
Local IP address/Mask	Router LAN IP address. It will be configured as the LAN IP automatically.	NULL
Remote IP Add Range	Remote VPN IP address range	
Broadcast Relay mode	Broadcast relay mode as Disabled, LAN to VPN client, VPN client to LAN, Both optional	Disable
Protocol Type	PPTP/L2TP Optional	PPTP
Encryption	None/MPPE-128 optional	None
DNS Servers	VPN Domain Name Resolution Server	0.0.0.0
WINS servers	VPN Domain Name Resolution Server which is based on 机的 NetBIOS of WIN OS.	0.0.0.0
MTU	Maximum Transmission Unit(MTU) for transmission traffic	1450
MRU	Maximum Transmission Unit(MTU) for receive traffic	1450

parameter	Instruction	Default
Custom Configuration	VPN Custom Configuration	NULL
PPTP/L2TP Client List	Configure VPN name, VPN static IP and VPN client LAN IP address/Mask	NULL

Step 2 Please click “save” to finish.



Configuration Instance

---End

2.11.7 PPTP/L2TP Client Setting

Step 1 VPN Tunnel> VPN Client to check or modify the relevant parameter.

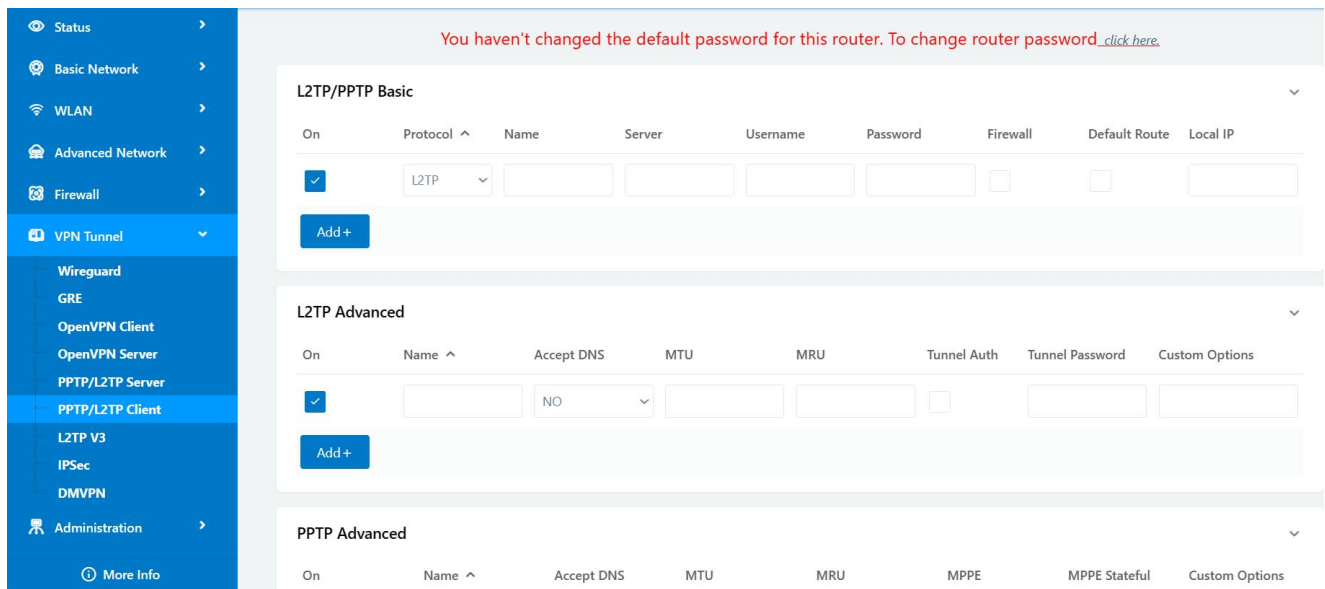


Table 2-31 PPTP/L2TP Basic Instruction

parameter	Instruction	Default
On	VPN enable	
Protocol	VPN Mode for PPTP and L2TP	
Name	VPN Tunnel name	
Server Address	VPN Server IP address.	
Username	As the configuration requested.	
Password	As the configuration requested.	
Firewall	Firewall For VPN Tunnel	

parameter	Instruction	Default
Local IP	Defined Local IP address for tunnel	

Table 2-32 L2TP Advanced Instruction

On	L2TP Advanced enable	
Name	L2TP Tunnel name	Default
Accept DNS	As the configuration requested.	
MTU	MTU is 1450bytes as default	
MRU	MRU is 1450bytes as default	
Tunnel Auth.	L2TP authentication Optional as the configuration requested.	
Tunnel Password	As the configuration requested.	
Custom Options	As the configuration requested.	

Table 2-33 PPTP Advanced Instruction

On	PPTP Advanced enable	Default
Name	PPTP Tunnel name	
Accept DNS	As the configuration requested.	
MTU	MTU is 1450bytes as default	
MRU	MRU is 1450bytes as default	
MPPE	As the configuration requested	
MPPE Stateful	As the configuration requested	
Customs	As the configuration requested	

Table 2-34 SCHEDULE Instruction

On	VPN SCHEDULE feature enable	Default
Name1	VPN tunnel name	
Name2	VPN tunnel name	
Policy	Support VPN tunnel backup and failover modes optional	

Description	As the configuration requested	
-------------	--------------------------------	--

Step 2 Please click “save” to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

---End

2.11.8 L2TP V3 Setting

Step 1 VPN Tunnel> L2TP V3 to check or modify the relevant parameter.

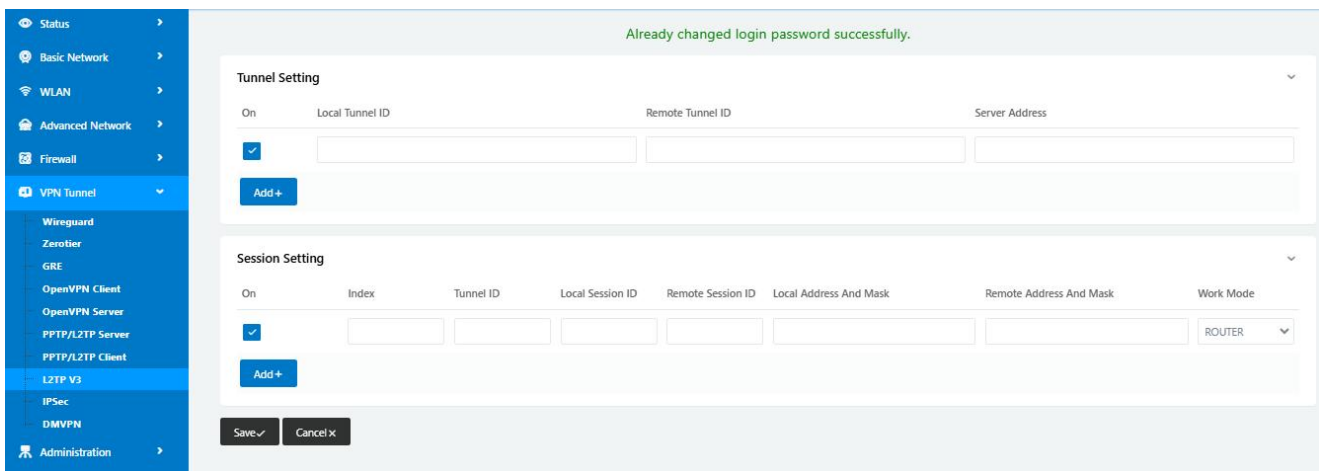


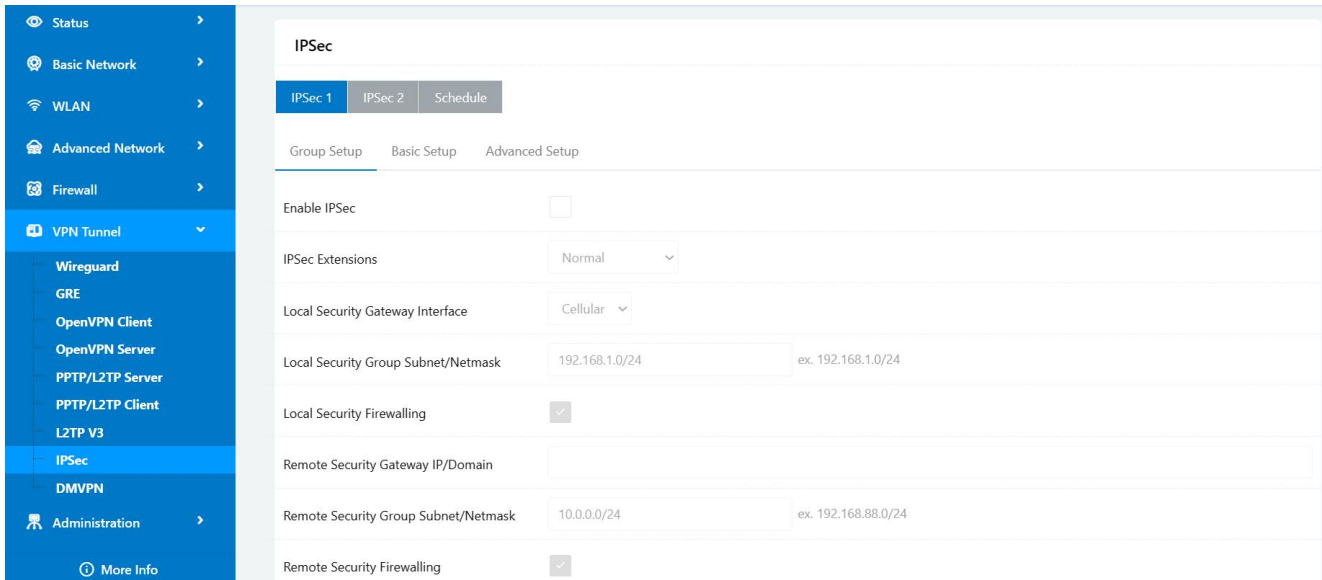
Table 2-35 L2TP V3 Basic Instruction

parameter	Instruction	Default
On	VPN on/off optional	OFF
Local Tunnel ID	Local VPN tunnel ID	NULL
Remote Tunnel ID	Remote VPN tunnel ID	NULL
Server Address	VPN Server IP address	NULL
Index	VPN sequence number	NULL
Tunnel ID	VPN tunnel ID	NULL
Local Session ID	Local Session ID	NULL
Remote Session ID	Local Session ID	NULL
Local IP and mask	Local tunnel IP and mask as format A.B.C.D/M	NULL
Remote IP and mask	Remote tunnel IP and mask as format A.B.C.D/M	NULL
Work Model	Router/Gateway/Bridge optional	NULL

Step 2 Please click “save” to finish.

---End

2.11.9 IPSec Setting



2.11.4.1 IPSec Group Setup

Step 1 IPSec> Group Setup to check or modify the relevant parameter.

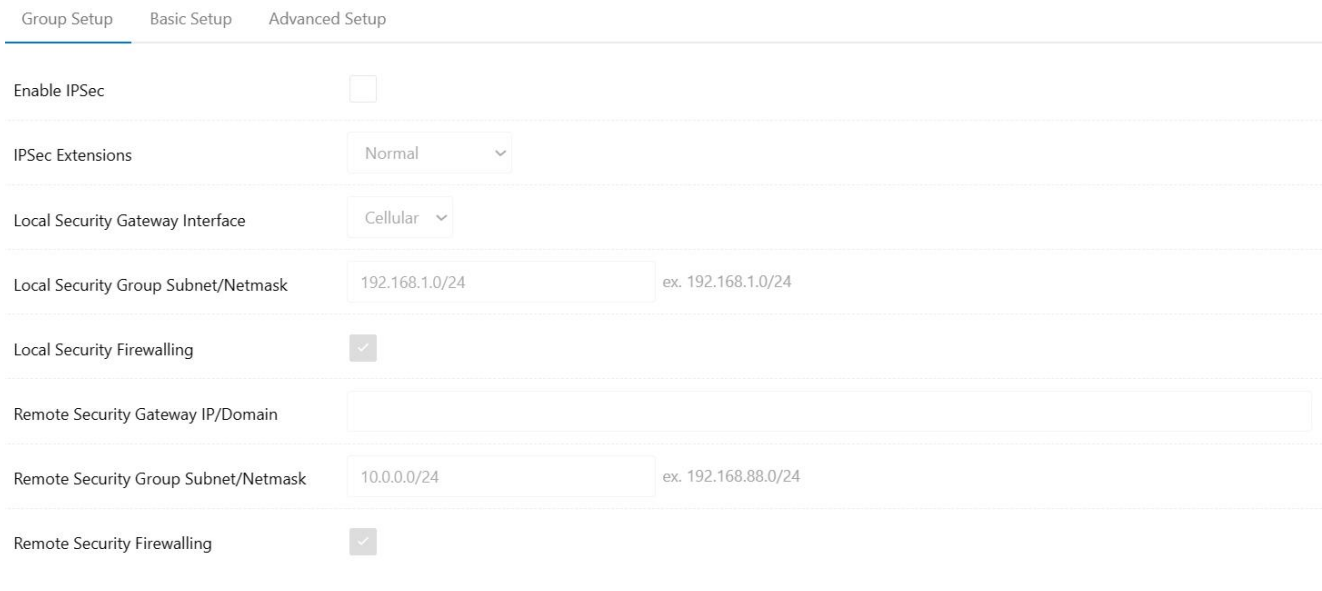


Table 2-36 IPSec Group Setup Instruction

Parameter	Instruction	Default
IPSec Extensions	Support Standard IPSec, GRE over IPSec, L2TP over IPSec	
Local Security Interface	Defined the IPSec security interface	

Parameter	Instruction	Default
Local Subnet/Mask	IPSec local subnet and mask.	
Local Firewall	Forwarding firewalling for Local subnet	
Remote IP/Domain	IPsec peer IP address/domain name.	
Remote Subnet/Mask	IPSec remote subnet and mask.	
Remote Firewall	Forwarding firewalling for Remote subnet	

Step 2 Please click “save” to finish.

--End

2.11.4.2 IPSec Basic Setup

Step 1 IPSec >Basic Setup to check or modify the relevant parameter.

Group Setup
Basic Setup
Advanced Setup

Keying Mode IKE ▾

Auth Mode Preshared Key ▾

Phase 1 DH Group Group 2 - modp1024 ▾

Phase 1 Encryption 3DES (168-bit) ▾

Phase 1 Authentication MD5 HMAC (96-bit) ▾

Phase 1 SA Life Time 28800 seconds

Phase 2 DH Group Group 2 - modp1024 ▾

Phase 2 Encryption 3DES (168-bit) ▾

Phase 2 Authentication MD5 HMAC (96-bit) ▾

Phase 2 SA Life Time 3600 seconds

Preshared Key

Table 2-37 IPSec Basic Setup Instruction

parameter	Instruction	Default
Keying Mode	IKE preshared key	
Phase 1 DH Group	Select Group1, Group2, Group5 from list. It must be matched to remote IPSec setting.	
Phase 1 Encryption	Support 3DES, AES-128, AES-192, AES-256	

parameter	Instruction	Default
Phase 1 Authentication	Support HASH MD5 and SHA	
Phase 1 SA Life Time	IPSec Phase 1 SA lifetime	
Phase 2 DH Group	Select Group1, Group2, Group5 from list. It must be matched to remote IPSec setting.	
Phase 2 Encryption	Support 3DES, AES-128, AES-192, AES-256	
Phase 2 Authentication	Support HASH MD5 and SHA	
Phase 2 SA Life Time	IPSec Phase 2 SA lifetime	
Preshared Key	Preshared Key	

Step 2 Please click “save” to finish.

---End

2.11.4.3 IPSec Advanced Setup

Step 1 IPSec >Advanced Setup to check or modify the relevant parameter.

Group Setup Basic Setup Advanced Setup

Aggressive Mode

Compress(IP Payload Compression)

Dead Peer Detection(DPD)

ICMP Check

IPSec Custom Options 1

IPSec Custom Options 2

IPSec Custom Options 3

IPSec Custom Options 4

Table 2-38 IPSec Advanced Setup Instruction

parameter	Instruction	Default
Aggressive Mode	Default for main mode	

parameter	Instruction	Default
ID Payload Compress	Enable ID Payload compress	
DPD	To enable DPD service	
ICMP	ICMP Check for IPSec tunnel	
IPSec Custom Options	IPSec advanced setting such as left/right ID.	

Step 2 Please click “save” to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

2.11.10 DMVPN Setting

Step 1 VPN Tunnel> DMVPN to check or modify the relevant parameter.

Table 2-39 DMVPN Basic Instruction

parameter	Instruction	Default
Enable	DMVPN enable/disable optional	OFF
Tunnel Address	GRE Tunnel IP address	NULL
Tunnel Mask	GRE Tunnel mask	NULL

parameter	Instruction	Default
Tunnel MTU	GRE Tunnel MTU	0
Tunnel Key	GRE Tunnel Key	NULL
Tunnel Source	Tunnel source IP address. Modem, WAN, sta, sta2 optional	NULL
NHRP Server Address	NHRP server IP address	NULL
NHRP Tunnel Address	NHRP Tunnel IP address	NULL
LNHRP Server Address2	LNHRP server IP address1	NULL
NHRP Tunnel Address2	RNHRP server IP address1	NULL
NHRP Key	NHRP Key	NULL
Keying Mode	IPsec key. IKE1 shared key and IKE2 shared key optional	
Phase 1 DH Group	Phase1 Group. Group1, 2,5 optional	
Phase 1 Encryption	3DES, AES-128/192/256 optional	
Phase 1 Authentication	MD5, SHA, SHA2 256/384/512 optional	
Phase 1 SA Life Time	Phase 1 SA Life available time	
Phase 2 DH Group	Phase1 Group. Group1, 2,5 optional	
Phase 2 Encryption	DES, AES-128/192/256 optional	
Phase 2 Authentication	MD5, SHA, SHA2 256/384/512 optional	
Phase 2 SA Life Time	Phase 2 SA Life available time	
Preshared Key	IPSec preshared key	
Dead Peer Detection(DPD)	Dead Peer Detection(DPD)	
IPSec Custom Options	IPSec Custom as requested	

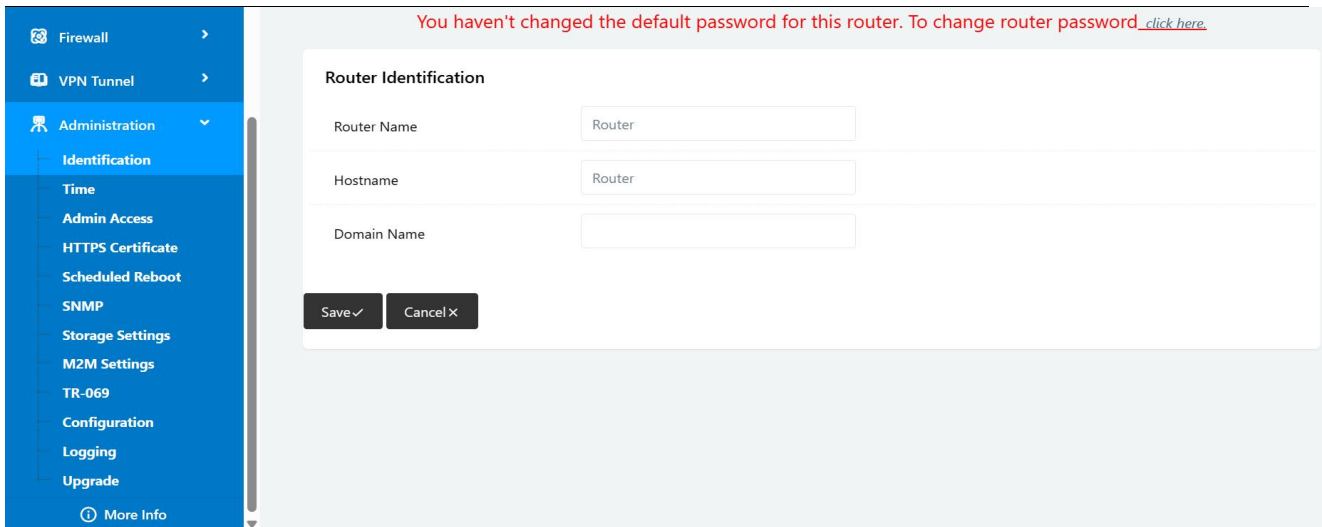
Step 2 Please click “save” to finish.

---End

2.12 Administration

2.12.1 Identification Setting

Step 1 Please click “Administrator” > “Identification” to enter the GUI, you may modify the router name, Host name and Domain name according to self-requirement.



Router Identification

Router Name

Hostname

Domain Name

Table 2-40 Router Identification Instruction

Parameter	Instruction	Default
Router name	Default is router, can be set maximum 32 character	
Host name	Default is router, can be set maximum 32 character	
Domain name	Default is empty, support maximum up to 32 characters, it is the domain of WAN, no need to configure for most application.	

Step 2 Please click “save” to finish.

----End

2.12.2 Time Setting

Step 1 Please click “Administrator> time” to check or modify the relevant parameter.

You haven't changed the default password for this router. To change router password [click here](#).

Time

Router Time Tue, 26 Mar 2024 10:43:50 +0800 Clock Sync.

Time Zone UTC+08:00 China, Hong Kong, Western Australia, Singapore, Taiwan

Auto Daylight Savings Time

Auto Update Time Every 4 Hours

Trigger Connect On Demand

NTP Time Server Asia

0.asia.pool.ntp.org, 1.asia.pool.ntp.org 2.asia.pool.ntp.org



If the device is online but time update is fail, please try other NTP Time Server.

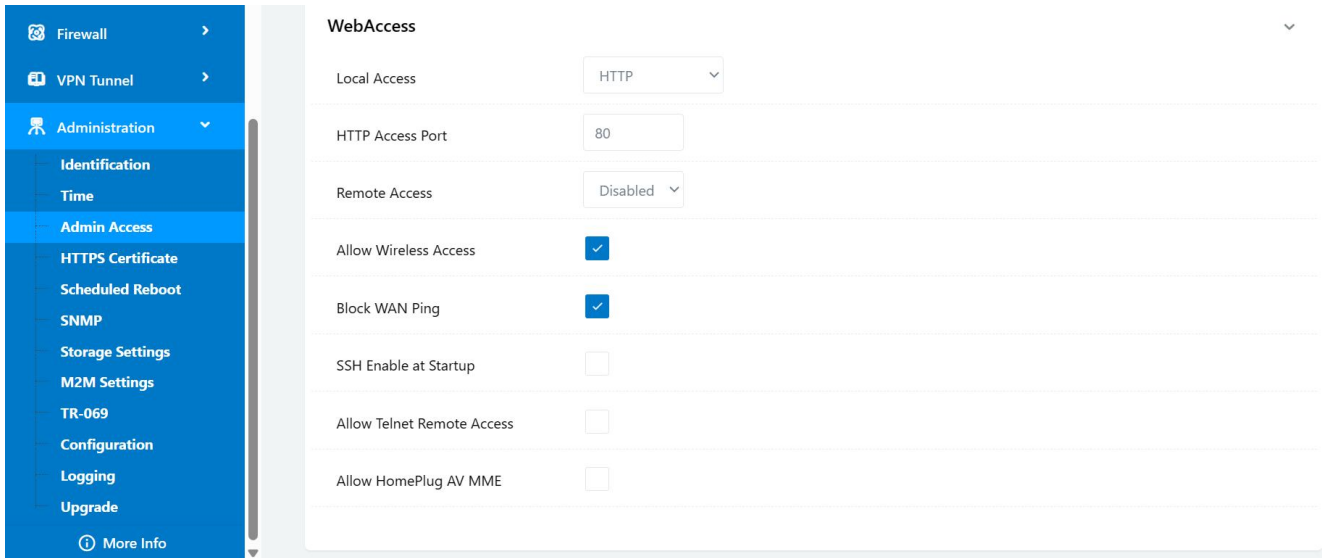
Step 2 Please click “save to finish.

----End

2.12.3 Admin Access Setting

Step 1 Please click “Administrator>Admin” to check and modify relevant parameter.

In this page, you can configure the basic web parameter, make it more convenient for usage. Please note the “password” is the router system account password.

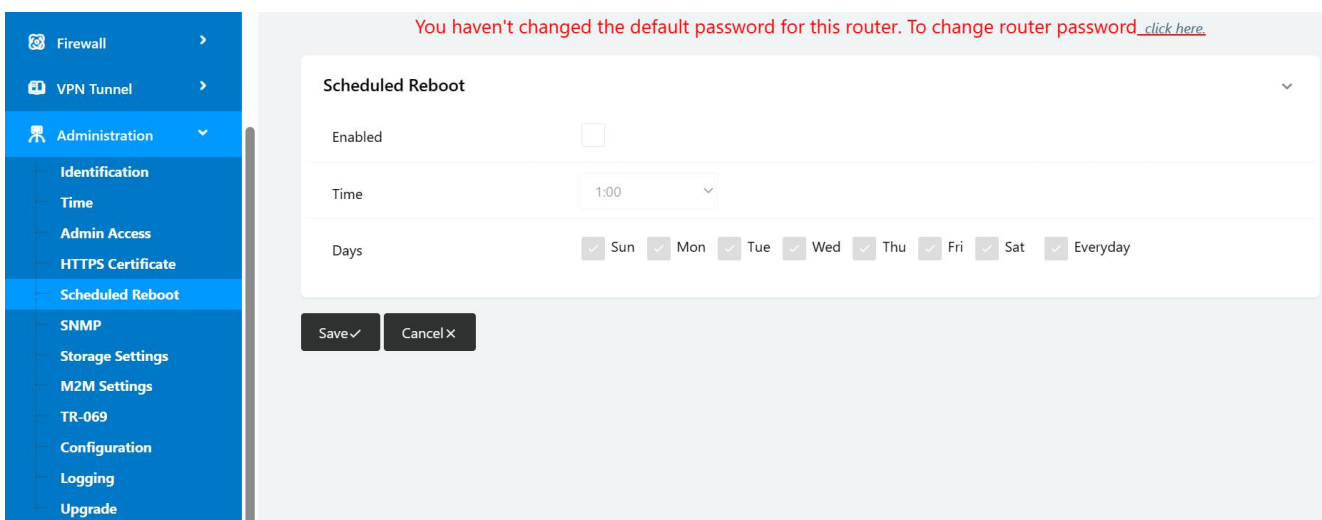


Step 2 Please click save icon to finish the setting.

----End

2.12.4 Schedule Reboot Setting

Step 1 Please click “Administrator>Schedule Reboot” to check and modify relevant parameter.

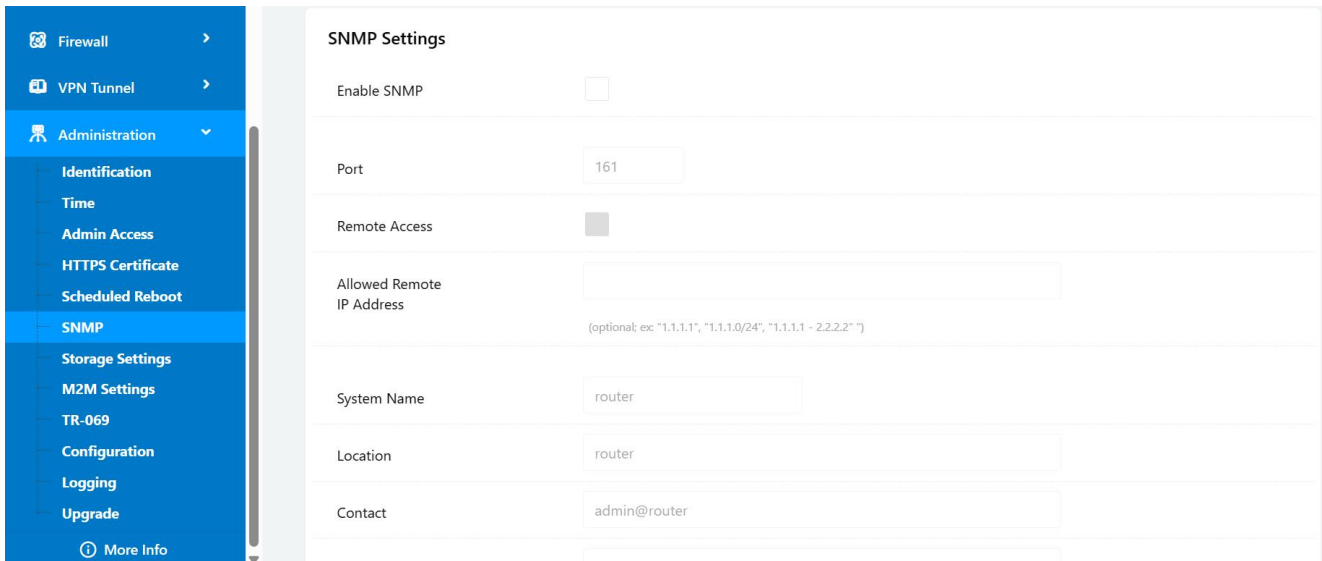


Step 2 Please click save icon to finish the setting.

----End

2.12.5 SNMP Setting

Step 1 Please click “Administrator>SNMP” to check and modify relevant parameter.

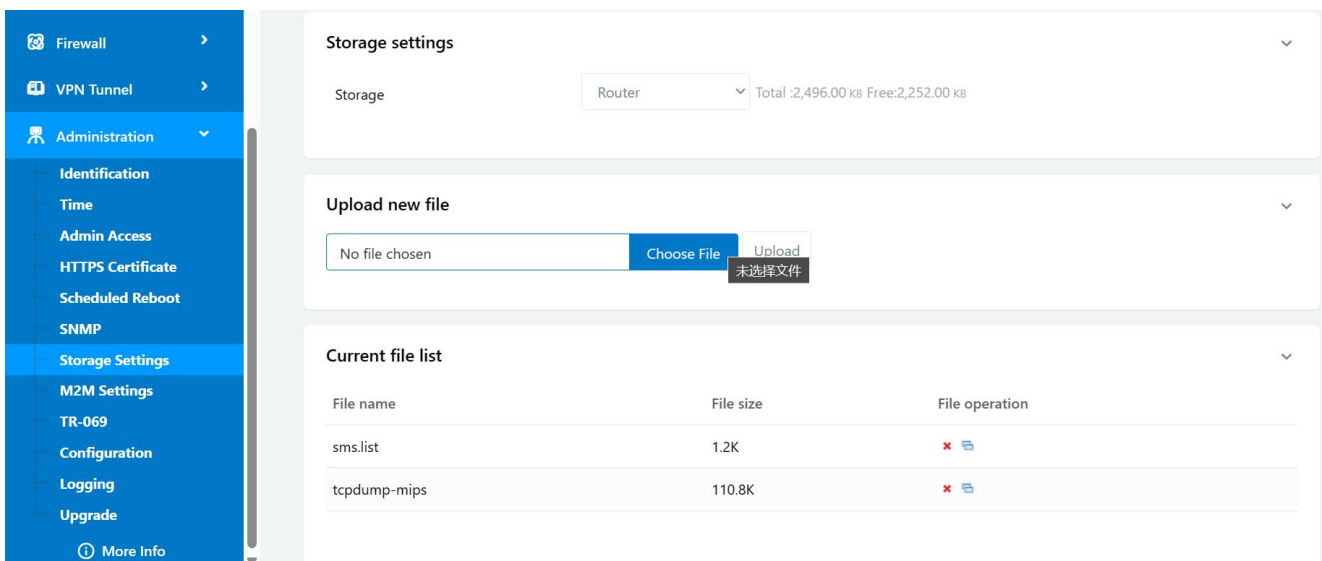


Step 2 Please click save icon to finish the setting.

----End

2.12.6 Storage Setting

Step 1 Please click “Administrator>Storage Setting” to check and modify relevant parameter.



Step 2 Please click save icon to finish the setting.

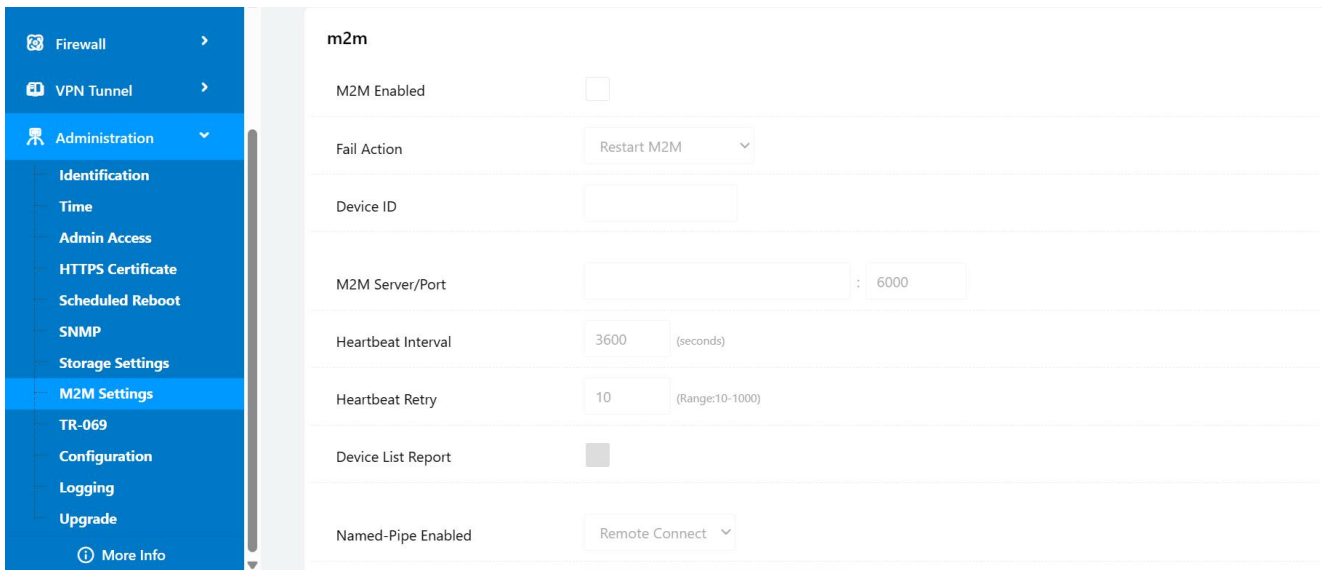


NOTE WL-R100/R200 series router doesn't support extra storage. The storage path is Router as default.

----End

2.12.7 M2M Access Setting (Apply to M2M Management Platform installation application only)

Step 1 Please click “Administrator>M2M Access” to check and modify relevant parameter.

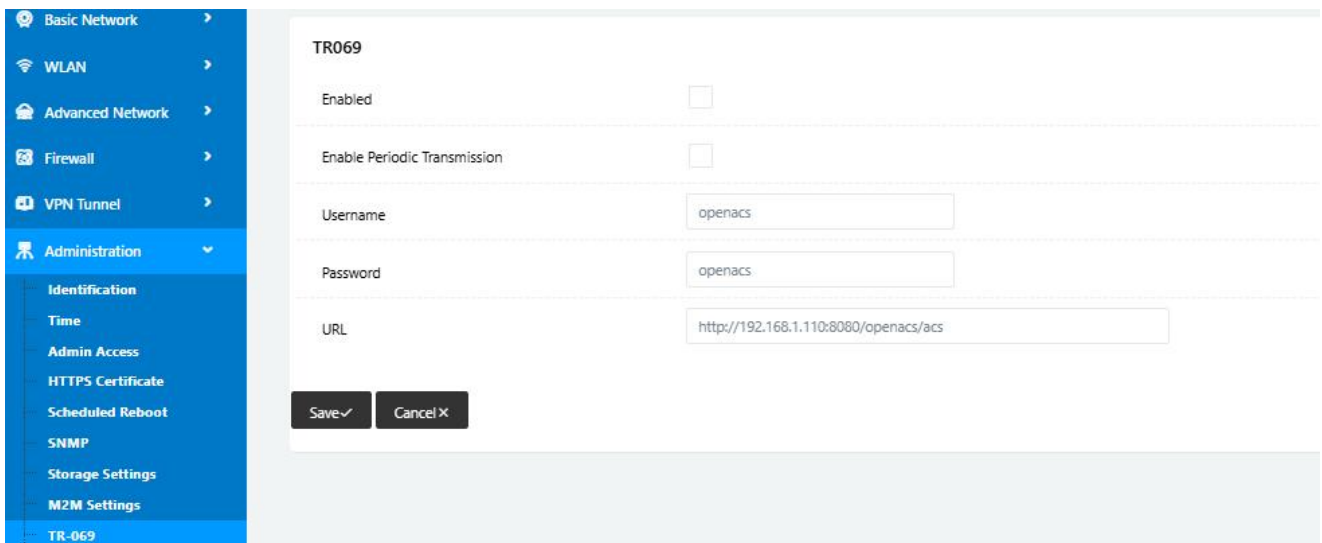


Step 2 Please click save iron to finish the setting.

----End

2.12.8 TR069

Step 1 Please click “Administrator>TR069” to check and modify relevant parameter.

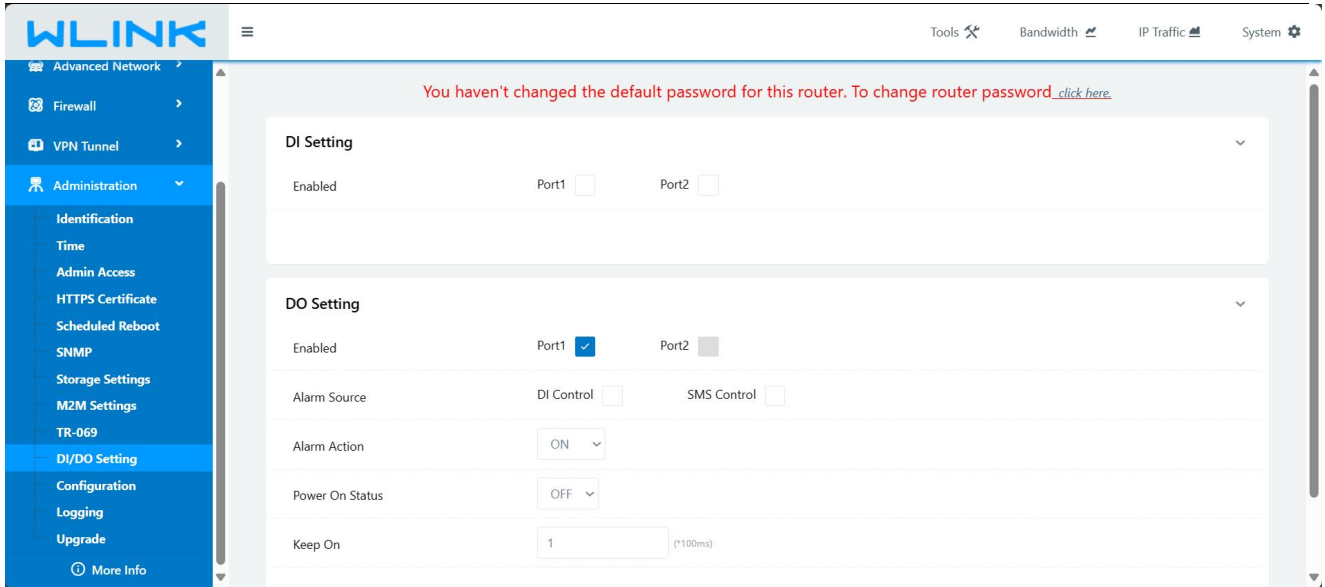


Step 3 Please click save iron to finish the setting.

----End

2.12.9 DI/DO Setting (Apply to WL-R210/R230 only)

Step 1 Please click “Administrator>DI/DO Setting” to check and modify relevant parameter.



2.12.8.1 DI Configure

DI Setting

Enabled	Port1 <input checked="" type="checkbox"/>	Port2 <input type="checkbox"/>
Port1Mode	<input type="text" value="ON"/>	
Filter	<input type="text" value="1"/> (*100ms)	
SMS Alarm	<input type="checkbox"/>	

DO Setting

Enabled	Port1 <input checked="" type="checkbox"/>	Port2 <input type="checkbox"/>
Alarm Source	DI Control <input type="checkbox"/>	SMS Control <input type="checkbox"/>
Alarm Action	<input type="text" value="ON"/>	
Power On Status	<input type="text" value="OFF"/>	
Keep On	<input type="text" value="1"/> (*100ms)	

Table 2-41 DI Instruction

Parameter	Instruction	Default
Enable	Enable DI. Port1 is for I/O1 and Port2 is I/O2. Both I/O1 and I/O2 are DI ports	
Mode	Selected from OFF, ON and EVENT_COUNTER modes. OFF Mode: DI from high level(3.3v~5V) to low level(0V), it will trigger alarm. ON Mode: DI from low level(0V) to high level(3.3v~5V), it will trigger alarm. EVENT_COUNTER Model: Enter EVENT_COUNTER mode.	
Filter	Software filtering is used to control switch bounces. Input (1~100)*100ms. Under OFF and ON modes, WL-G510 detects pulse signal and compares with first pulse shape and last pulse shape. If both are the same level, WL-G510 will trigger alarm. Under EVENT_COUNTER mode, if first pulse shape and last pulse shape are not the same level, WL-G510 will trigger alarm according to Counter Action setting.	
Counter Trigger	Available when DI under Event Counter mode Input from 0 to 100. (0=will not trigger alarm) It will trigger alarm when counter reaches this value. After triggering alarm, DI will keep counting but no trigger alarm again.	
Counter Period	It's a reachable IP address. Once the ICMP check is failed, GRE will be established again.	
Counter Recover	it will re-count after counter trigger alarm. The value is 0~30000(*100ms). 0 means no counter.	
Counter Action	HI_TO_LO and LO_TO_HI is available when DI under Event Counter mode. In Event Counter mode, the channel accepts limit or proximity switches and counts events according to the ON/OFF status. When LO_TO_HI is selected, the counter value increase when the attached switch is pushed. When HI_TO_LO is selected, the counter value increases when the switch is pushed and released.	
Counter Start	Available when DI under EVENT_COUNTER mode. Start counting when enable this feature.	
SMS Alarm	The alarm SMS will send to specified phone group.	

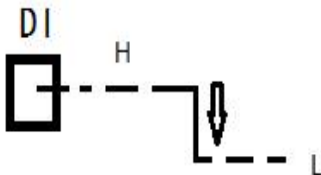
Parameter	Instruction	Default
	Each phone group include up to 2 phone numbers.	
SMS Content	70 ASCII Char Max	
Number 1	SMS receiver phone number.	
Number 2	SMS receiver phone number.	

Step 2 Please click “save” to finish.



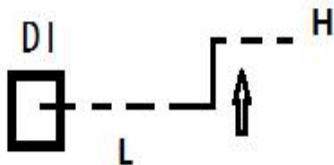
OFF Mode

DI from high level 3.3~5V to low level 0V will be triggered.



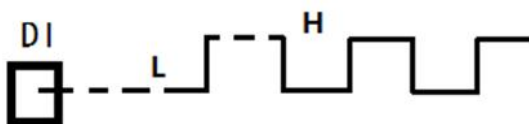
ON Mode

Data input from low level 0V to high level 3.3~5V will be triggered.



EVENT_COUNTER Model

The counted number of pulses will be triggered.



2.12.8.2 DO Configure

DO Setting

Enabled Port1 Port2

Alarm Source DI Control SMS Control

Alarm Action

Power On Status

Delay (*100ms)

Low (*100ms)

High (*100ms)

Output

Keep On (*100ms)

SMS Trigger Content
70 ASCII Max

SMS Reply Content
70 ASCII Max

SMS admin Num1

SMS admin Num2 Backup

Table 2-42 DO Instruction

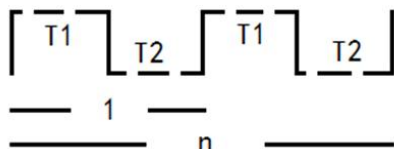
Parameter	Instruction	Default
Enable	1 DO as selected	
Alarm Source	Digital output initiates according to different alarm source. Select from DI Alarm, SMS Control and M2M Control. Selections can be one or more. DI Alarm: Digital Output triggers the related action when there is alarm from Digital Input. SMS Control: Digital Output triggers the related action when receiving SMS from the number in phone book. M2M Control: it's not ready.	
Alarm Action	Digital Output initiates when there is an alarm. Selected from "OFF", "ON", "Pulse". OFF: Open from GND when triggered. ON: Short contact with GND when triggered. Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.	
Power on Status	Specify the digital Output status when power on. Selected from OFF and ON. OFF: how high(0V). ON: high lever(4.8-5.0V)	

Parameter	Instruction	Default
Keep On	Available when digital output Alarm On Action/Alarm Off Action status is ON, input the Digital Output keep on status time. Input from 0 to 255 seconds. (0=keep on until the next action)	
Delay	Available when enable Pulse in Alarm On Action/Alarm Off Action. The first pulse will be generated after a “Delay” . Input from 0 to 30000ms. (0=generate pulse without delay)	
Low	Available when enable Pulse in Alarm On Action/Alarm Off Action. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low level widths are specified here. Input from 1 to 30000 ms.	
High	Available when enable Pulse in Alarm On Action/Alarm Off Action. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The high level widths are specified here. Input from 1 to 30000 ms.	
Output	Available when enable Pulse in Alarm On Action/Alarm Off Action. The number of pulses, input from 0 to 30000. (0 for continuous pulse output)	
SMS Trigger Content	Available when enable SMS Control in Alarm Source. Input the SMS content to enable “Alarm On Action” by SMS (70 ASIC II char max).	
SMS Reply Content	Input the SMS content, which will be sent after DO was triggered. (70 ASIC II char max).	
Number 1	SMS receiver phone number.	
Number 2	SMS receiver phone number.	

Step 3 Please click “save” to finish.



DO might be customized pulse width ratio: T1, T2 duration and n value.



---End

2.12.10 Configuration Setting

Step 4 Please click “Administrator > Configuration” to do the backup setting.

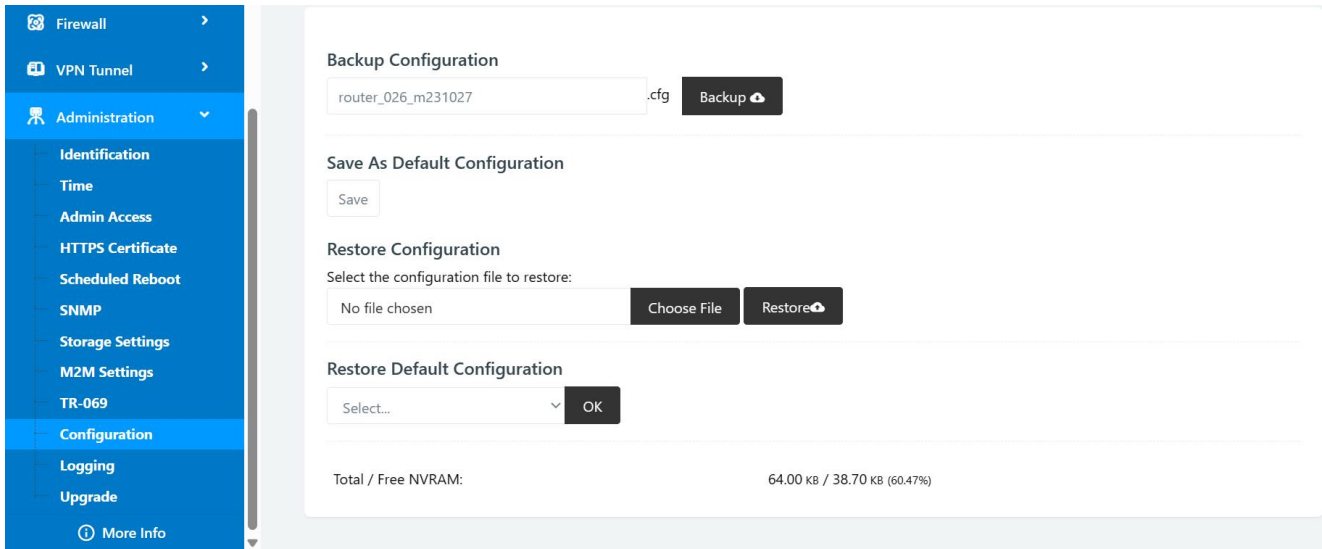


Figure 3-1 Backup and Restore Configuration GUI



Restore Default would lose all configuration information, please be careful.

Step 5 After setting the backup and restore configuration. The system will reboot automatically.

----End

2.12.11 System Log Setting

Step 6 Please click “Administrator> Logging” to start the configuration, you can set the file path to save the log (Local or remote sever).

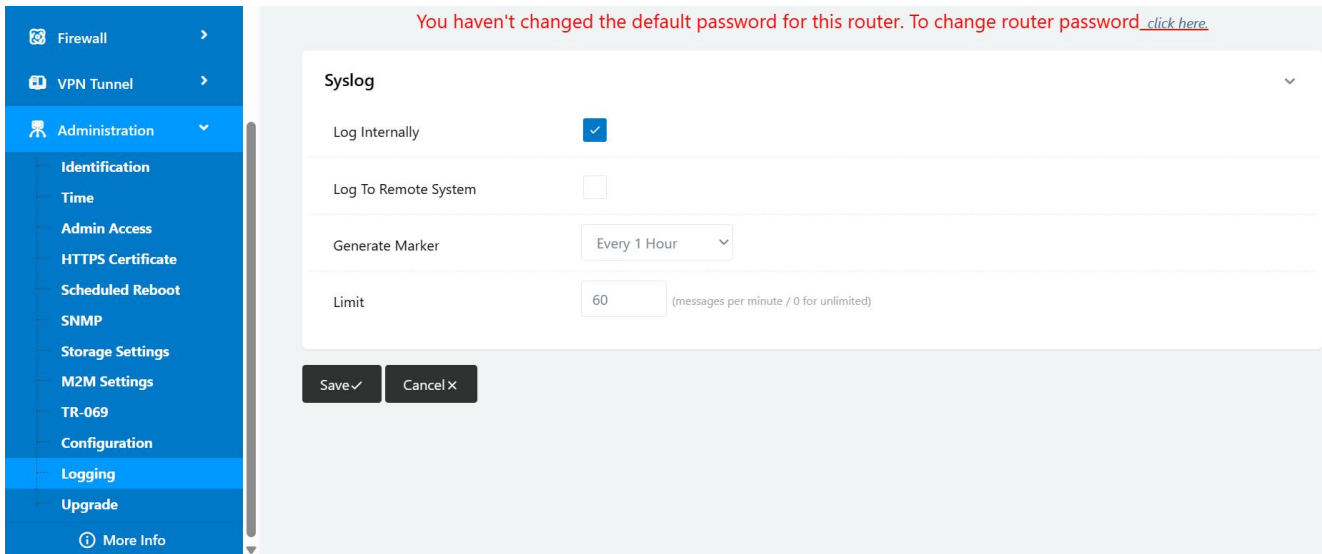


Figure 3-2 System log Setting GUI

Step 7 After configuring, please click “Save” to finish.

----End

2.12.12 Firmware upgrade

Step 8 Please click “Administrator>firmware upgrade” to open upgrade firmware tab.

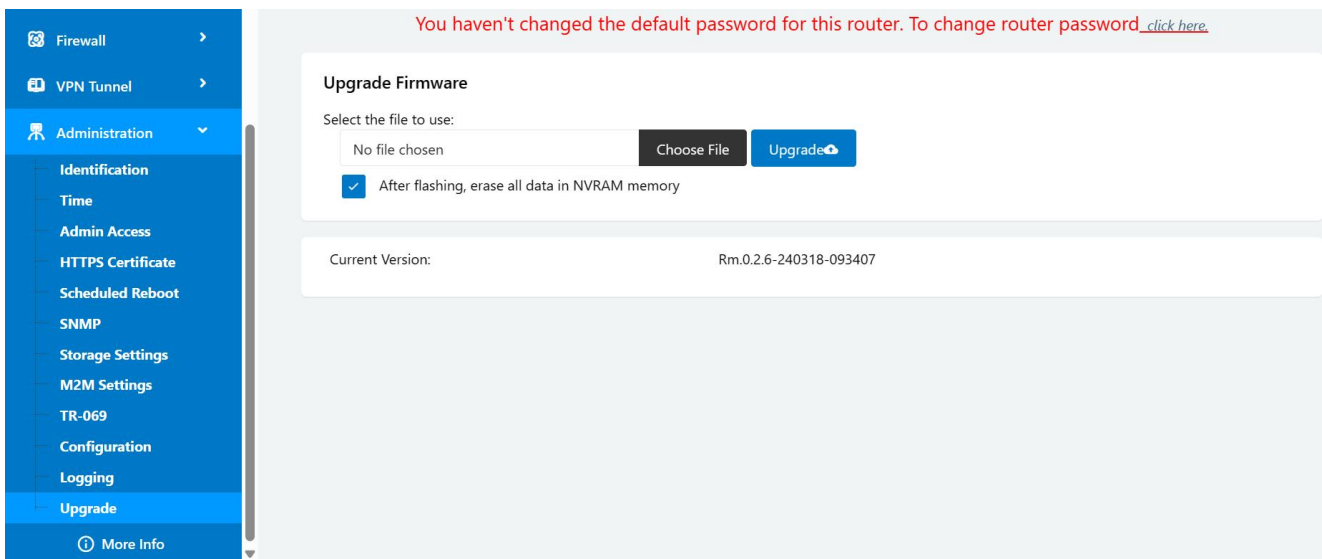


Figure 3-3 Firmware Upgrade GUI



Please don't cut off the power during upgrading. The upgrade period is about 4mins.

2.12.13 “Reset” Button for Restore Factory Setting

If you couldn't enter web interface for other reasons, you can also use this way. “Reset” button is near to Console port in WL-Rxx panel, This button can be used when the router is in use or when the router is turned on. Press the “RST” button and keep more than 8 seconds till the NET light stopping blink. The system will be reverted to factory.

Table 2-43 System Default Instruction

Parameter	Default setting	
LAN IP	192.168.1.1	
LAN Subnet Mask	255.255.255.0	
DHCP server	Enable	
Username	admin	
Password	admin	



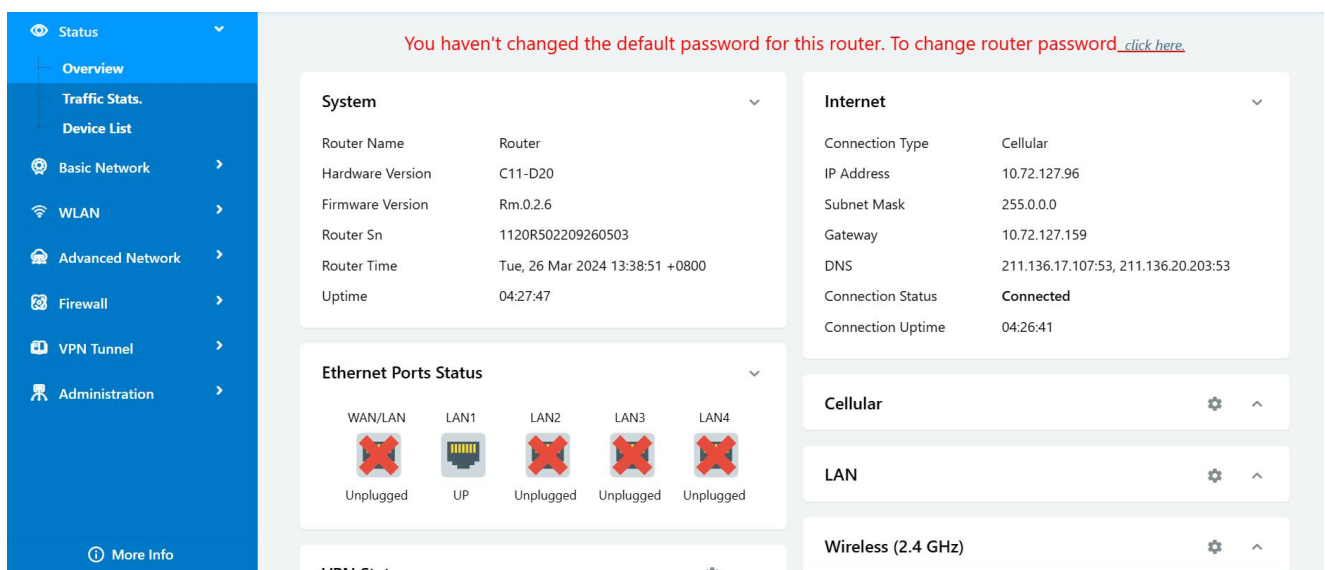
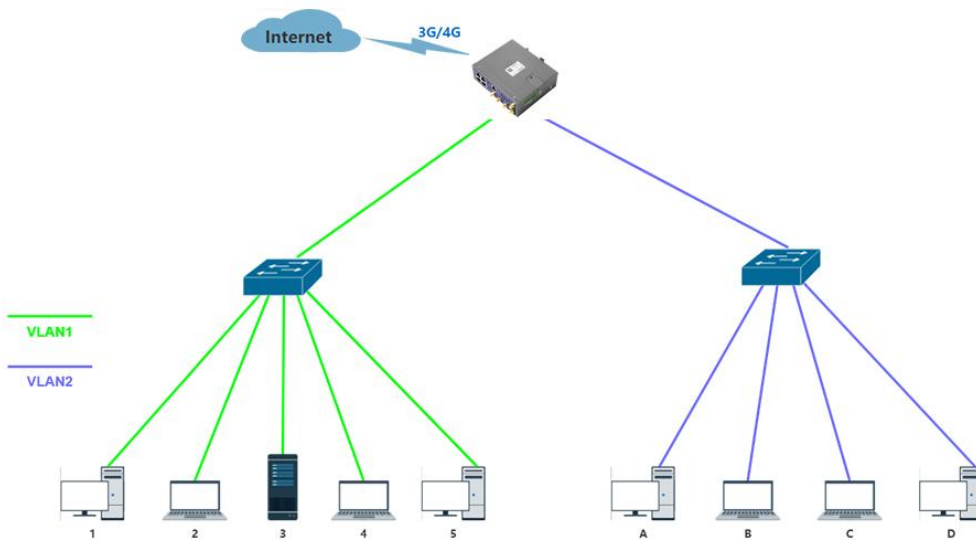
After reboot, the previous configuration would be deleted and restore to factory settings.

3 Configuration Instance

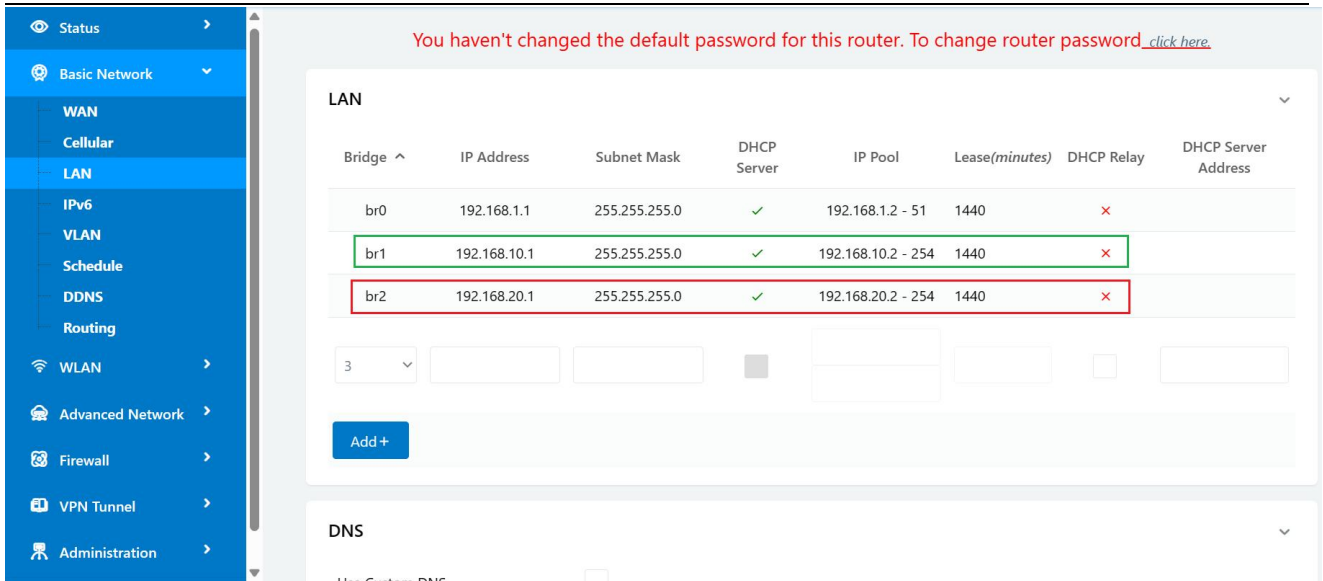
This chapter is mainly for configured test case, there would be some difference between the scheme and real object. But the difference doesn't have any influence to products performance.

3.1 VLAN

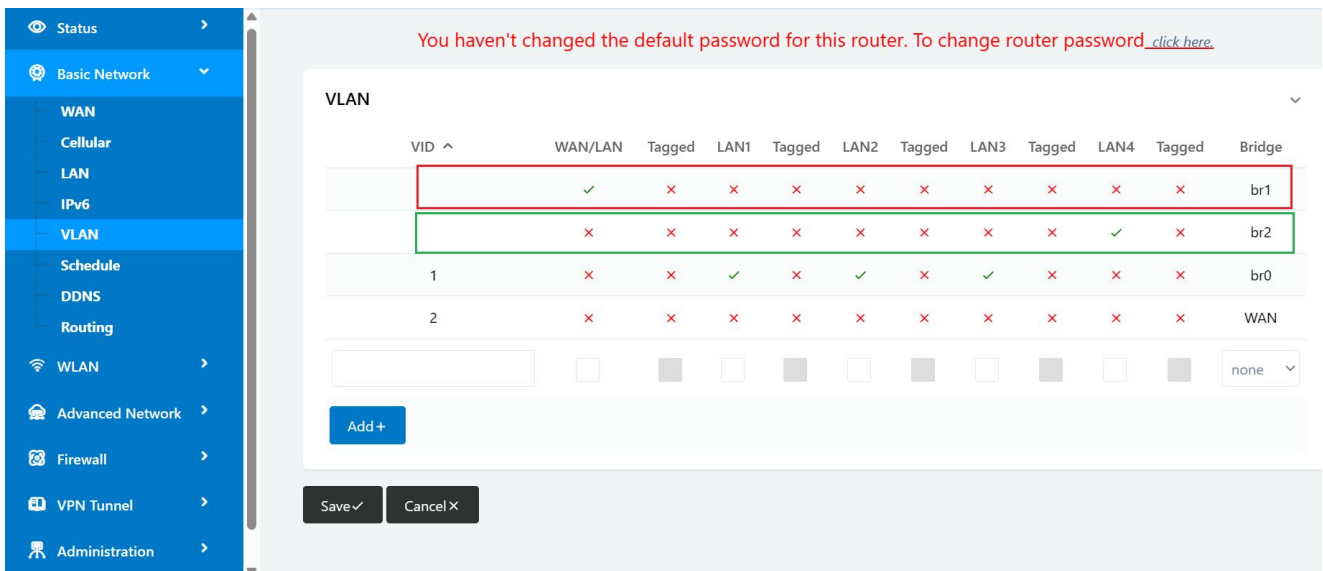
WL-R200/R210/R520 supports VLAN partition based on Ethernet port (LAN1~LAN5)



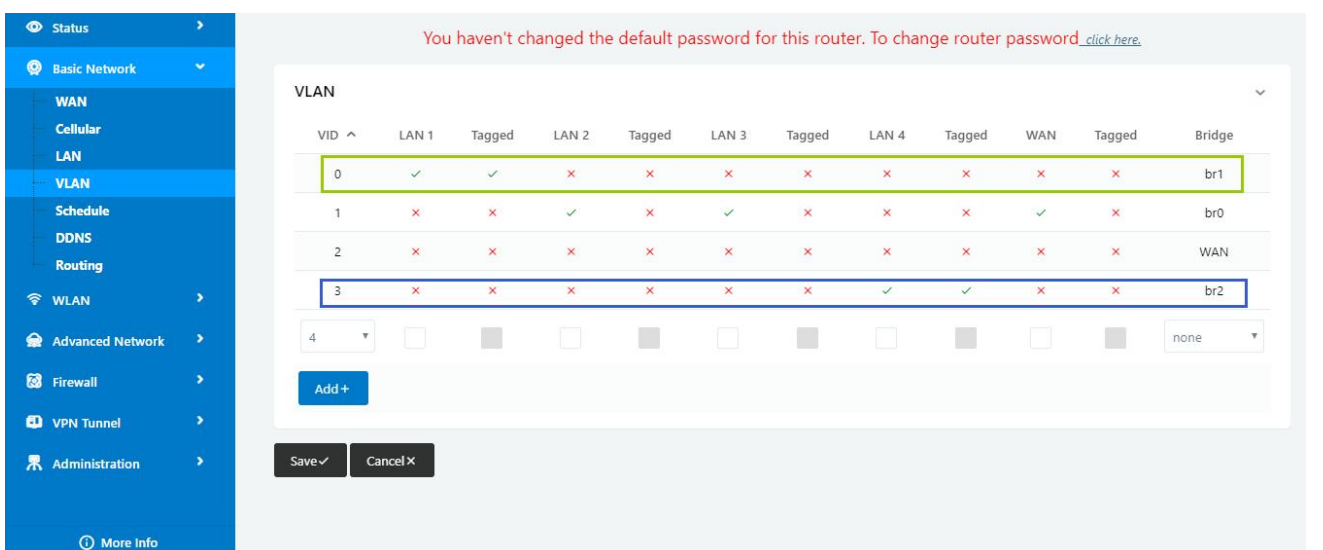
1) Configure LAN with Basic Network.



2) If untag for br1 and br2, it won't be accessed between SW1 and SW2.



3) If tag for br1 and br2, it will be accessed between sw1 and sw2.

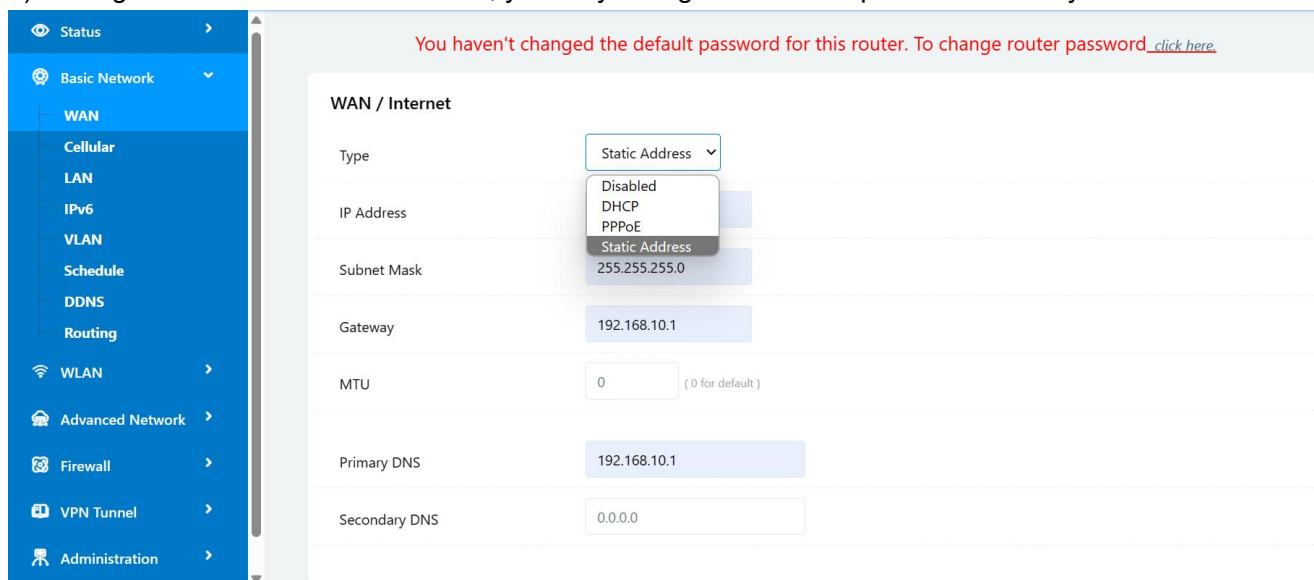


--End

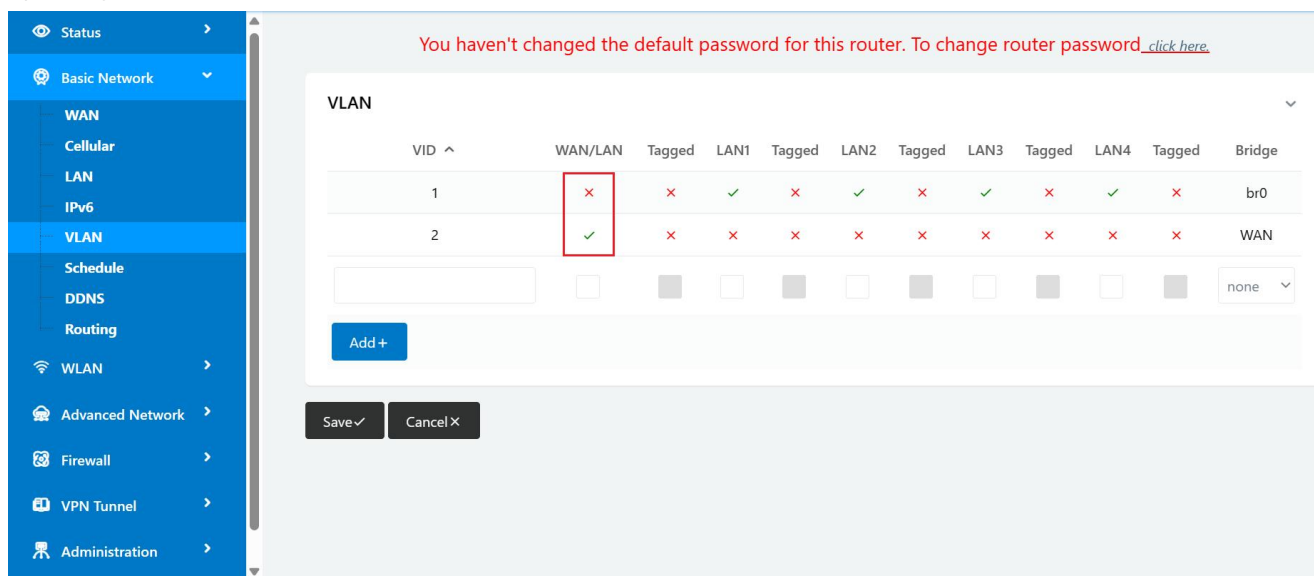
3.2 WAN Backup (WAN as Main, Cellular Backup)

The WAN and Cellular backup feature can quickly switch traffic to Cellular (link2) when WAN (link1) fails, and WL-Rxx brings you a stable network experience.

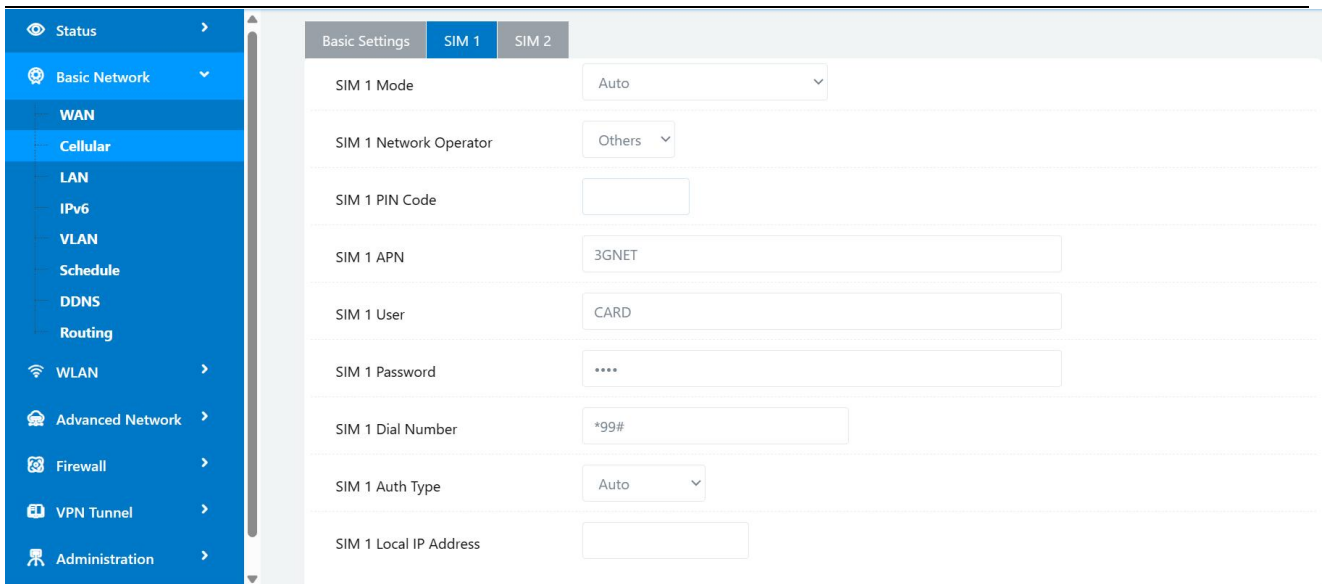
1) Navigate to Basic **Network > WAN**, you may configure the WAN parameters with your situation.



2) Navigate to **Basic Network > VLAN**, enable the LAN1 as WAN Ethernet



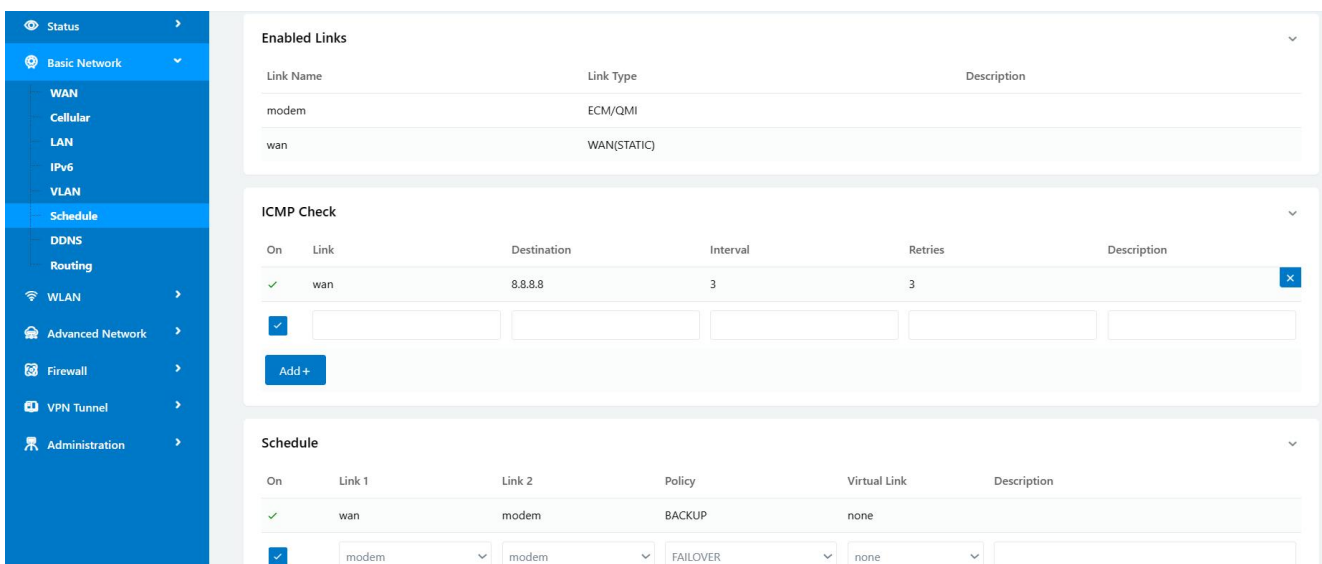
3) Navigate to **Basic network > Cellular**, configure the APN as your SIM



4) Navigate to **Basic Network > Schedule**, configure WAN (Link1) preferred, Cellular backup (Link2)

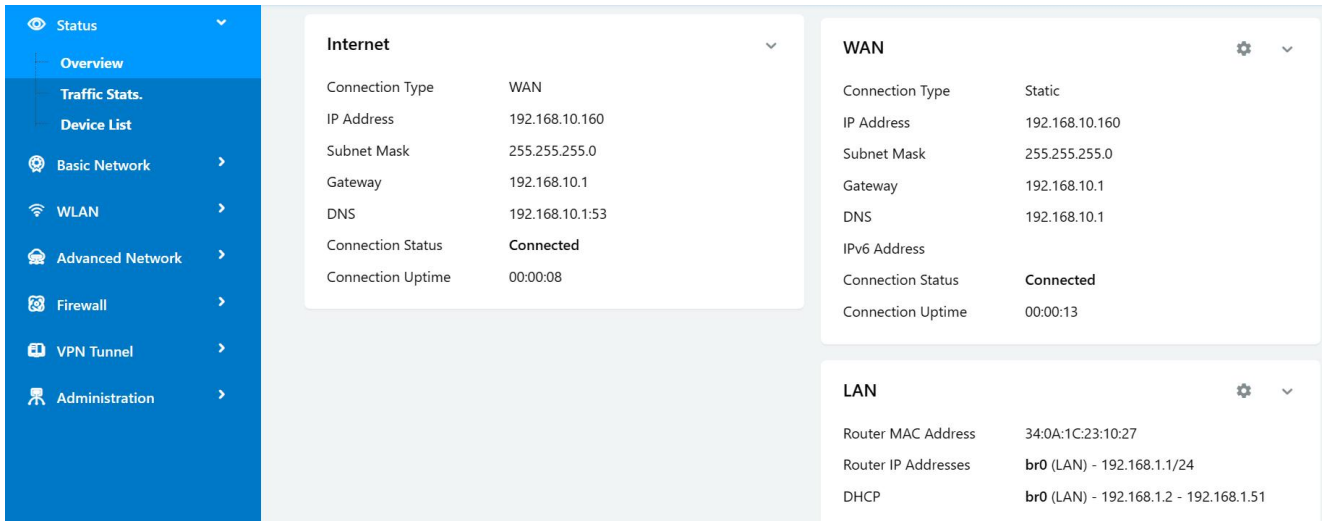
Add ICMP Check to WAN

Set the working mode (Schedule)



Parameters	Instruction	Default
modem	The router dial-up to network via modem	
wan	The router dial-up to network via WAN (DHCP, PPPOE, Static IP) Ethernet	
ICMP Check	When the ICMP Check fails, the switching action between Link 1 and Link2 will be triggered	
Link1	The preferred link	
Link2	The alternate link	
BACKUP	Backup mode, Link1 and Link2 will remain online at the same time	
FAILOVER	Failover mode, Link2 will dial-up to network when link1 fails	

5) Status: WAN working



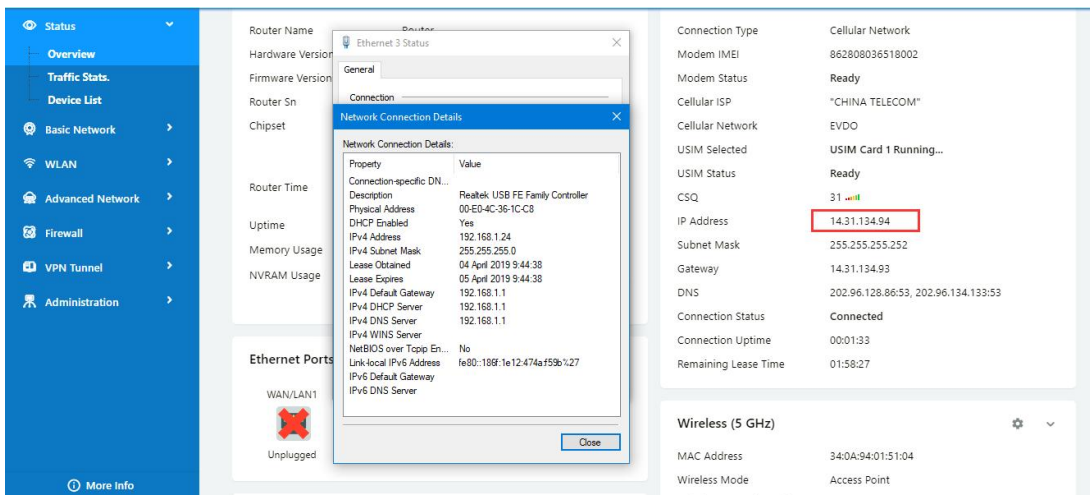
6) The system quickly switches traffic to Cellular when the WAN fails
---End

3.3 Port Forwarding

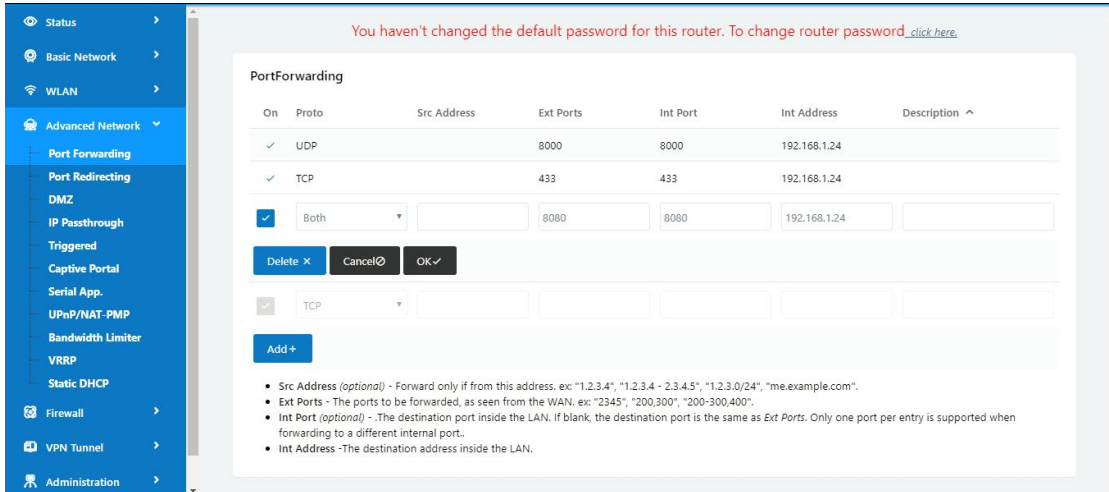
1) The router online and got a public IP address 14.31.134.94

Note: It's based on SIM card carrier

2) The PC is connected to router and got IP address 192.168.1.24



3) Configuration

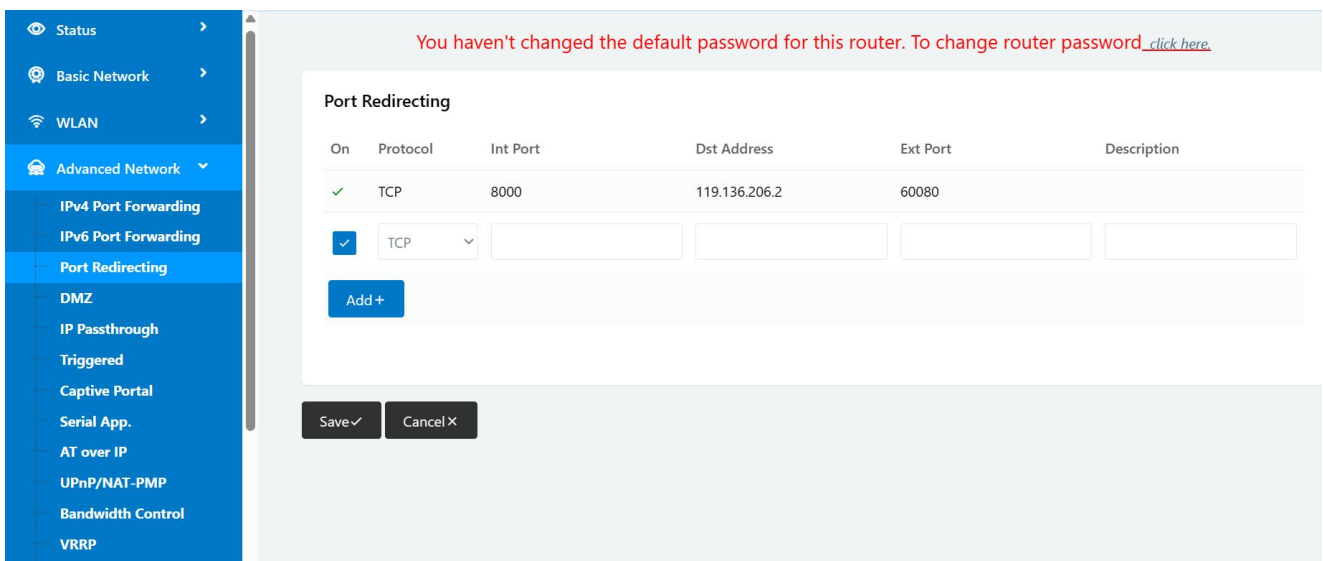


4) The PC can be accessed via 14.31.134.94:443 over Internet

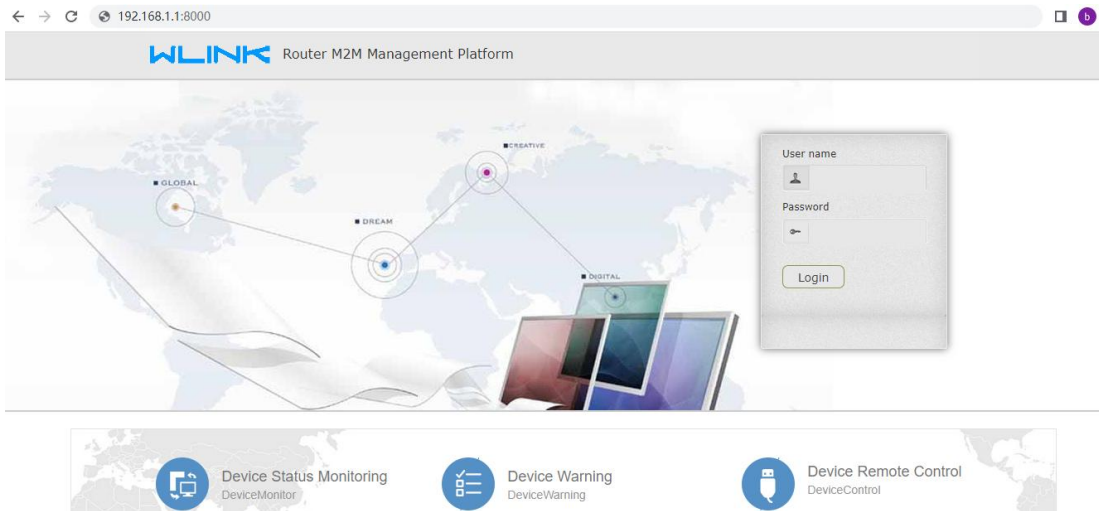
---End

3.4 Port Redirecting

Please click “Advanced Network> Port Redirecting” to check or modify the relevant parameter.



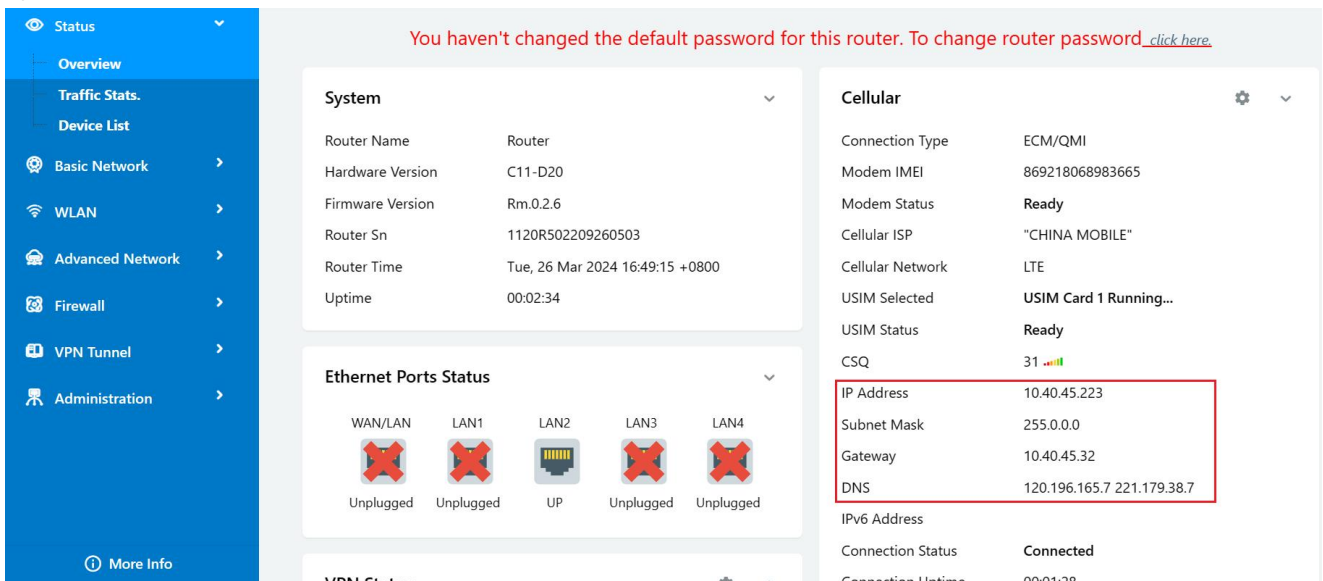
Configure Internal port as 8000, the Destination IP address as 119.136.206.2 and External port 60080(M2M Platform Server IP and Port as example). Access to 192.168.1.1:8000 in browser, the router will redirect to 119.136.206.2: 60080.



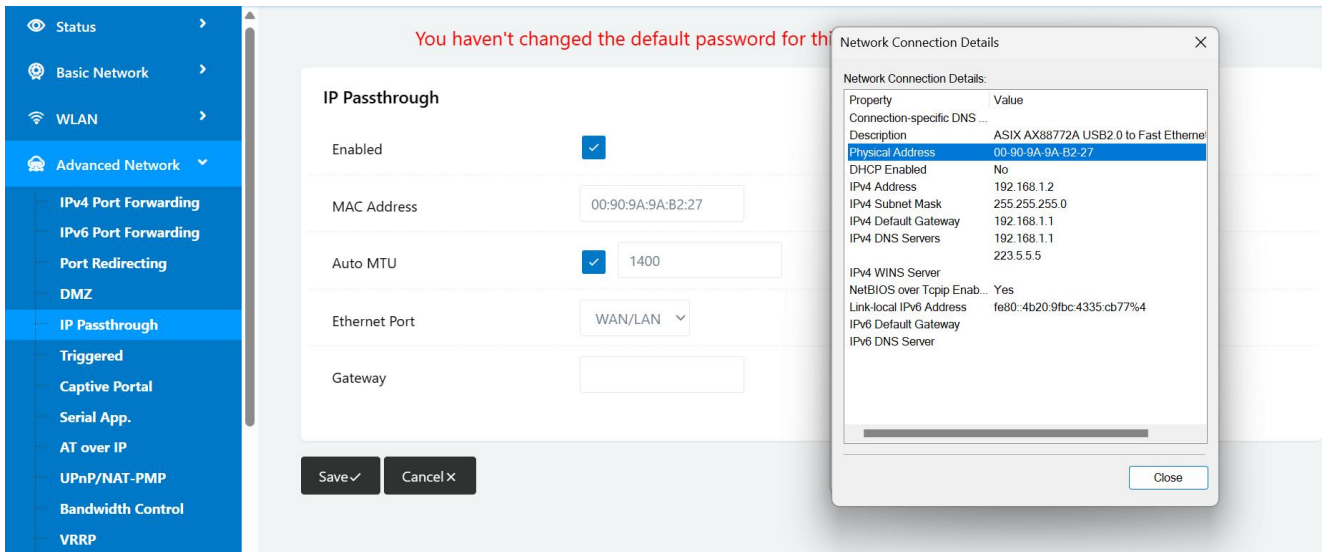
---End

3.5 IP Passthrough

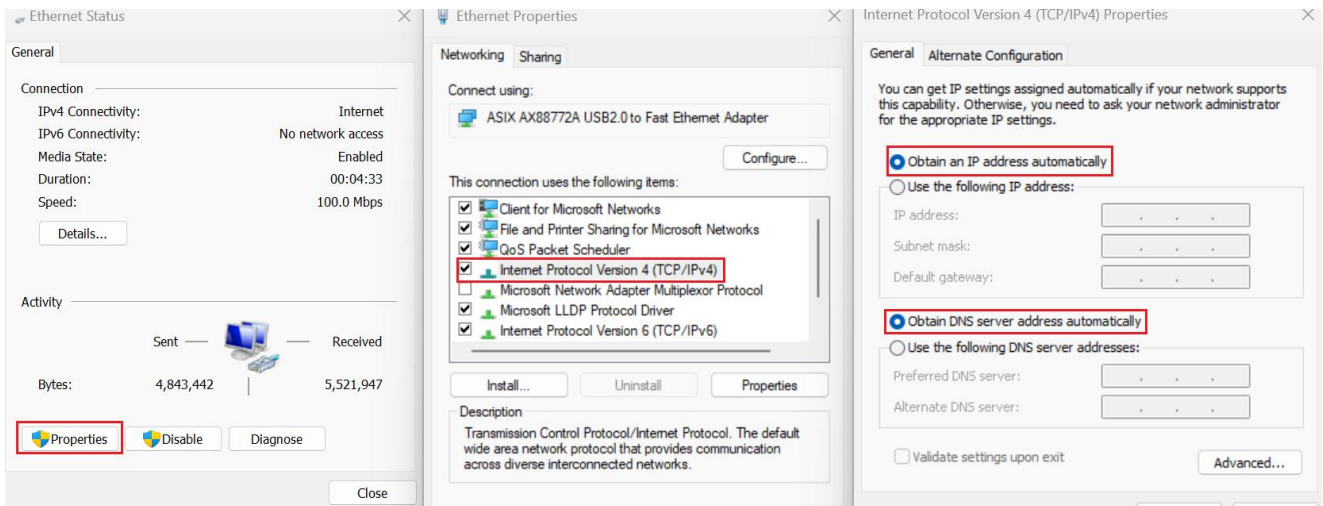
1) The router online



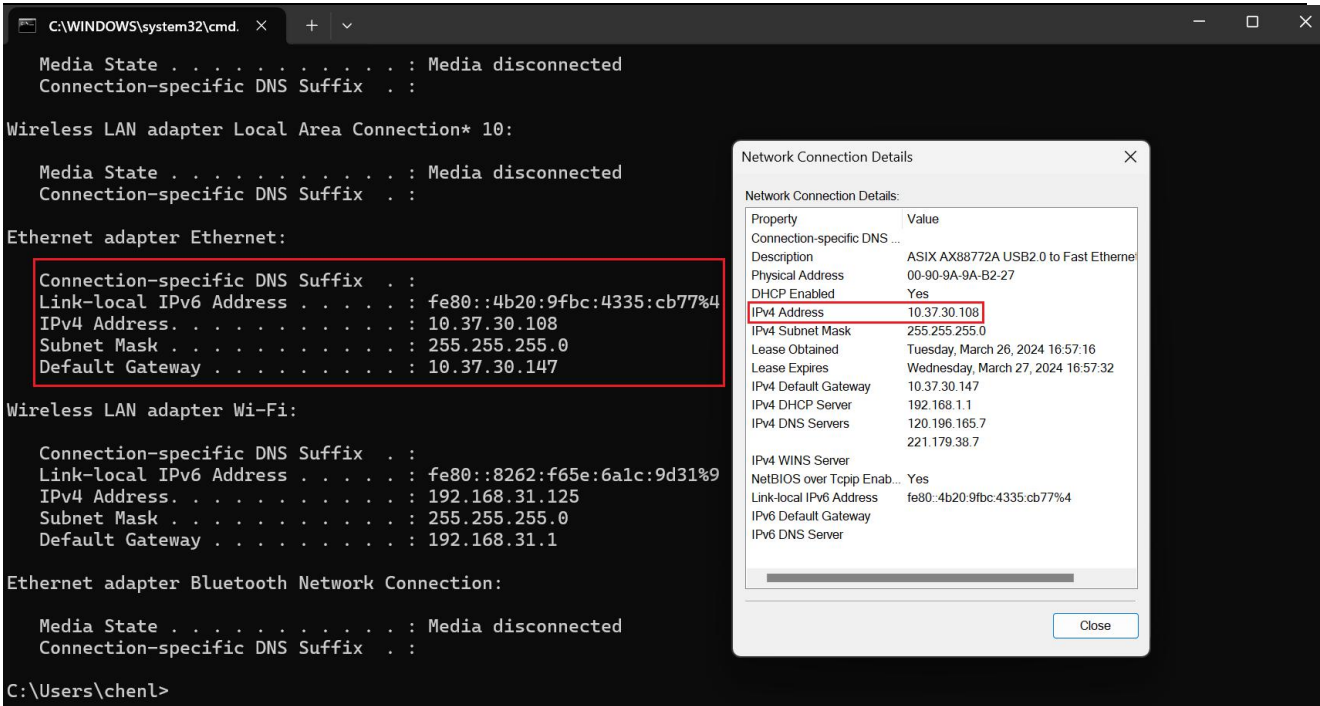
2) Configure IP passthrough destination MAC address (PC Ethernet MAC)



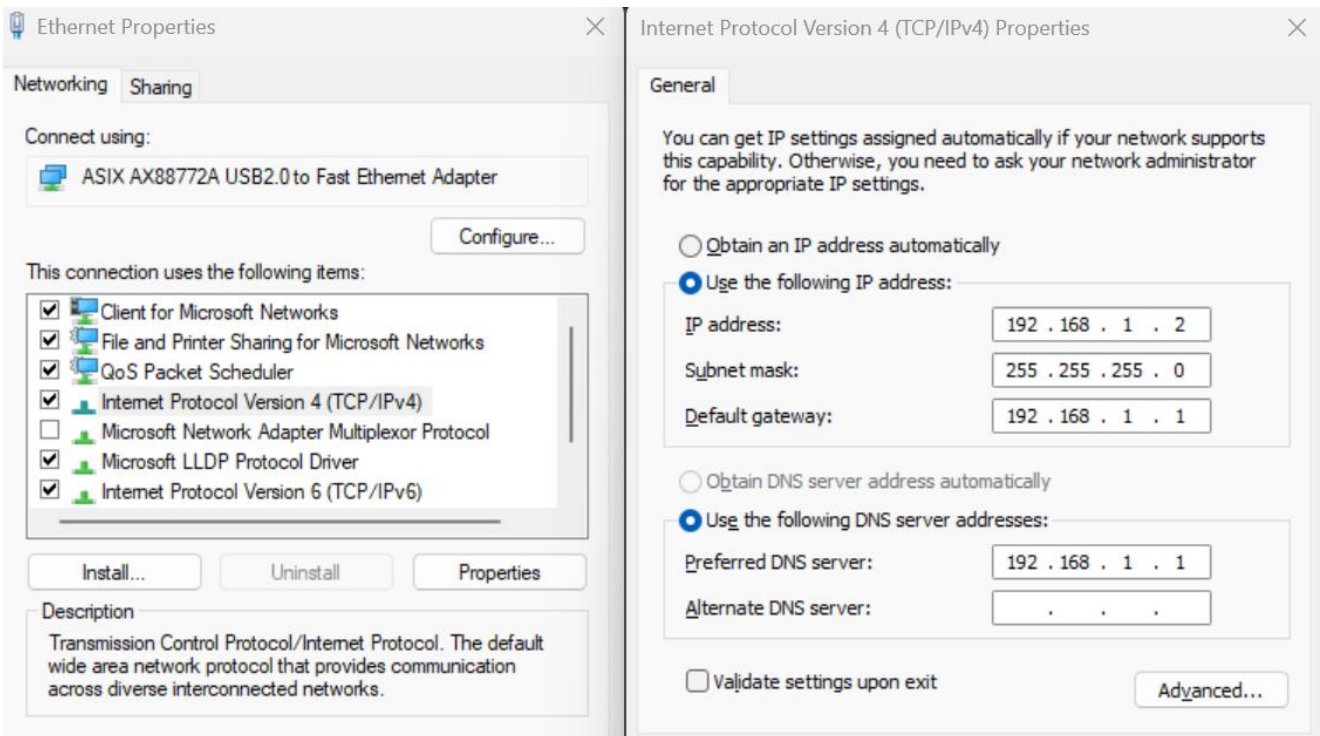
3) Set the PC to DHCP



4) Check the Ethernet status and ping test



5) Set the PC Ethernet as DHCP to release the IP and access to router GUI again

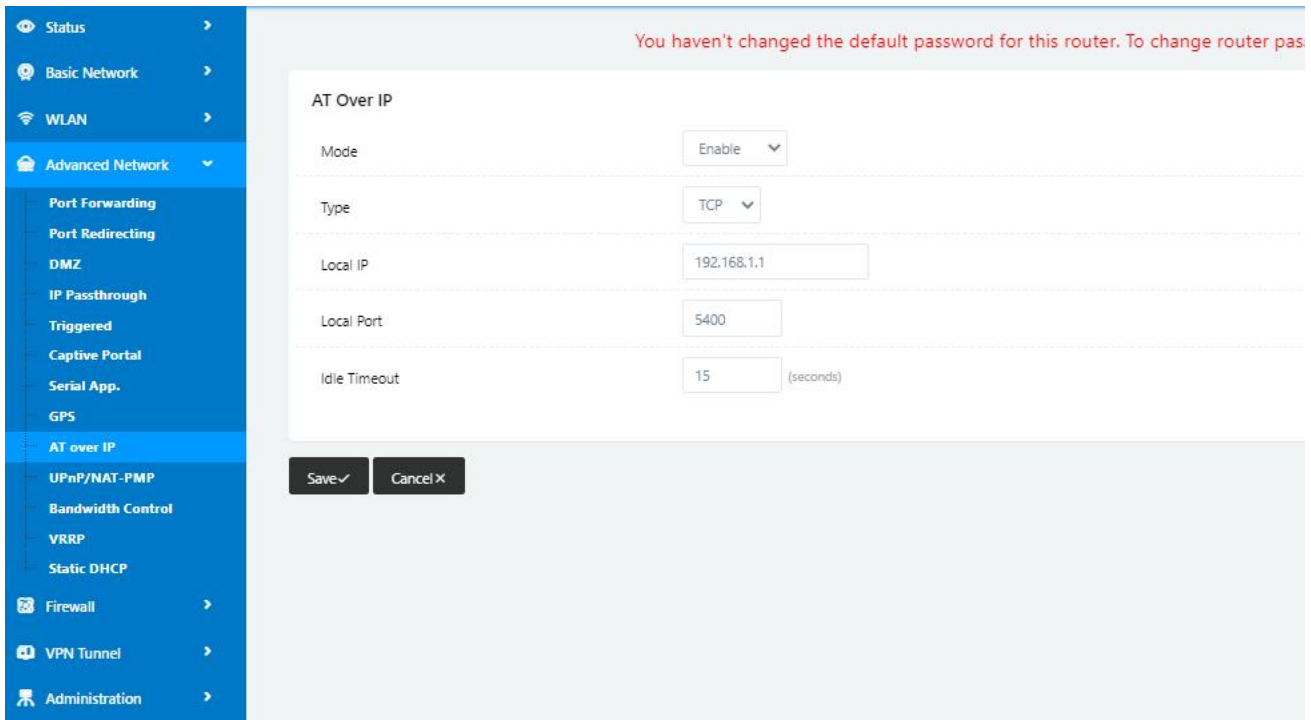


---End

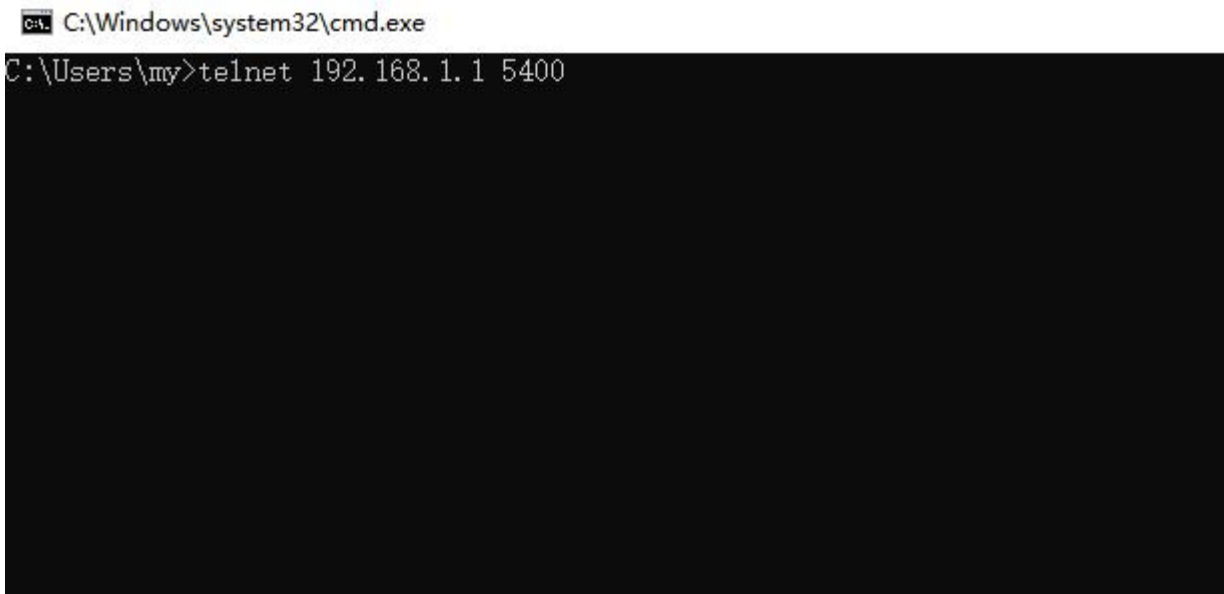
3.6 AT over IP

Please click “Advanced Network> AT over IP” to check or modify the relevant parameter.

Enable AT over IP Setting.



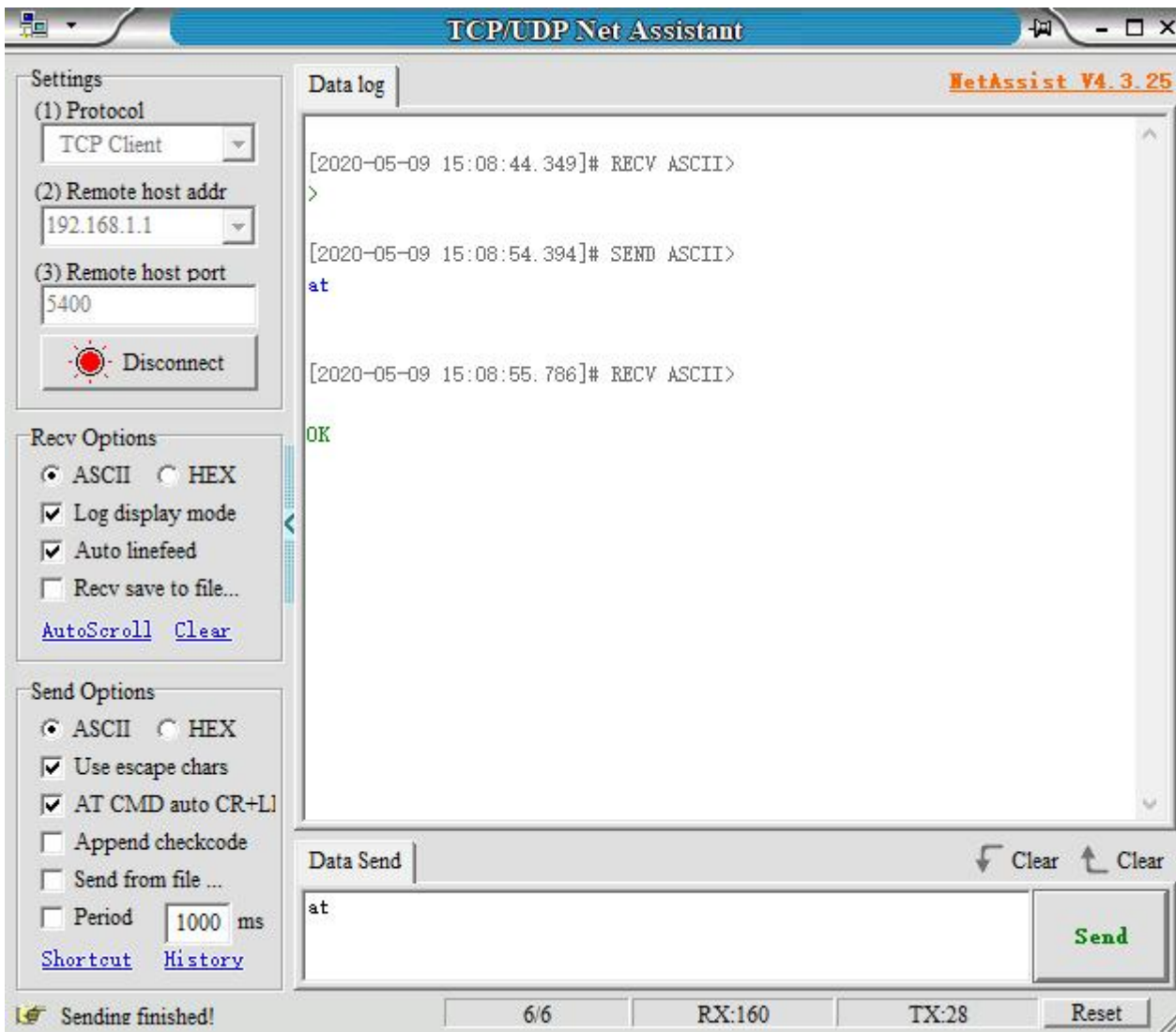
1) Access AT mode by Telnet

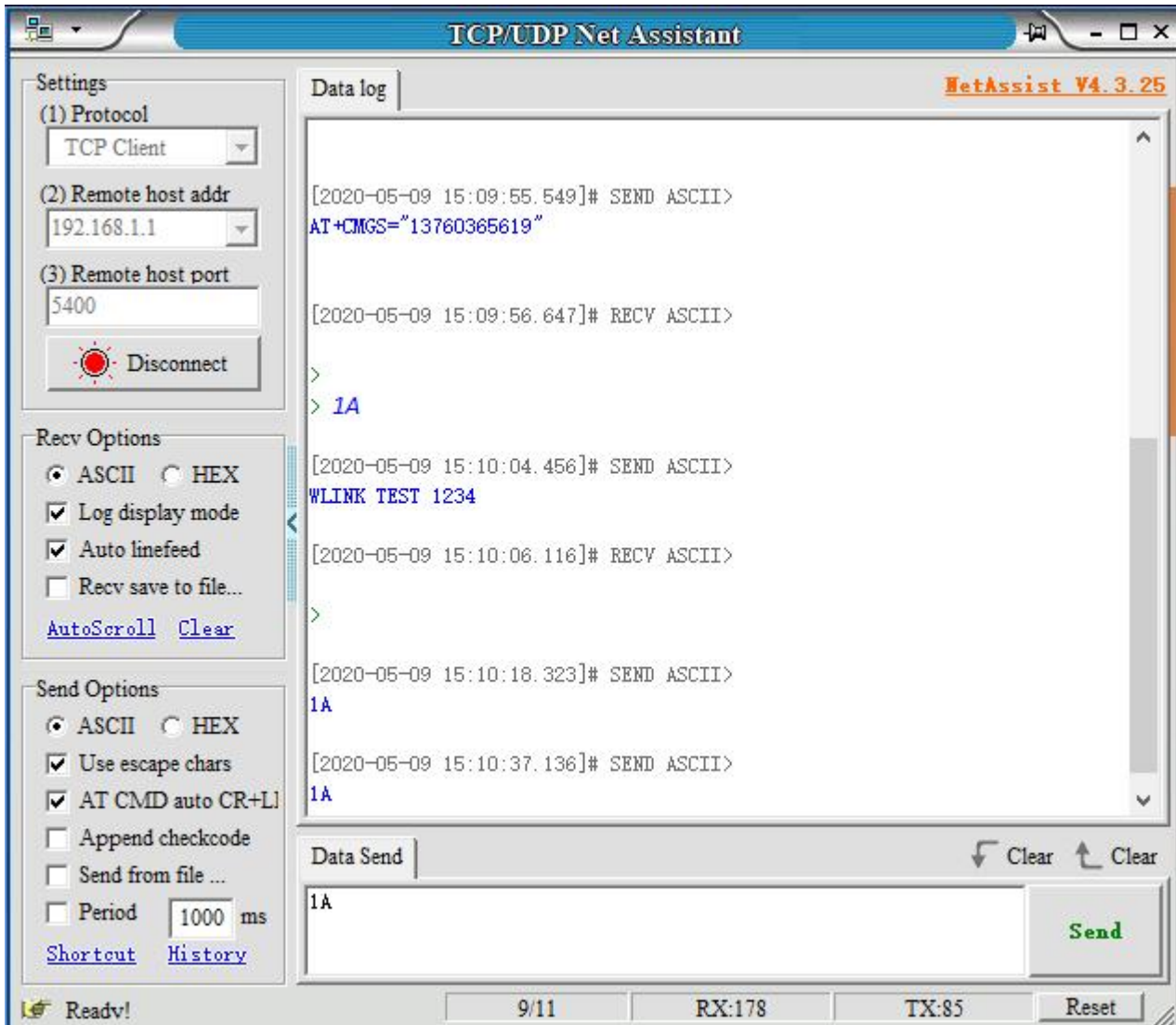


Implement AT command



2) Access AT mode via TCP Tool

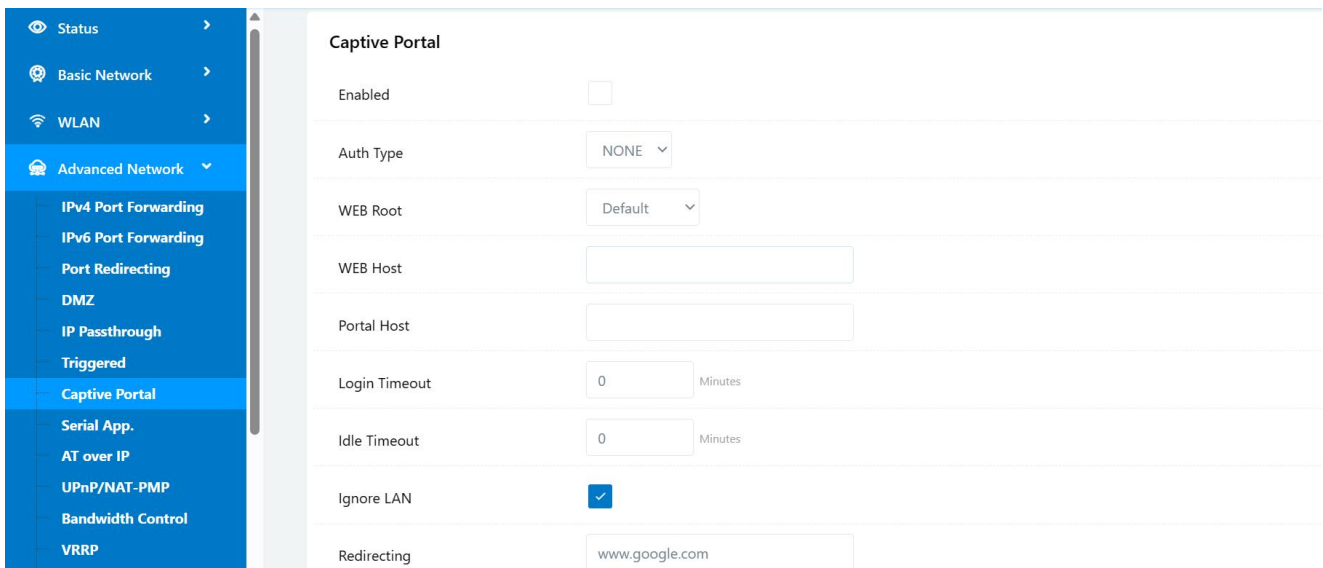




---End

3.7 Captive Portal

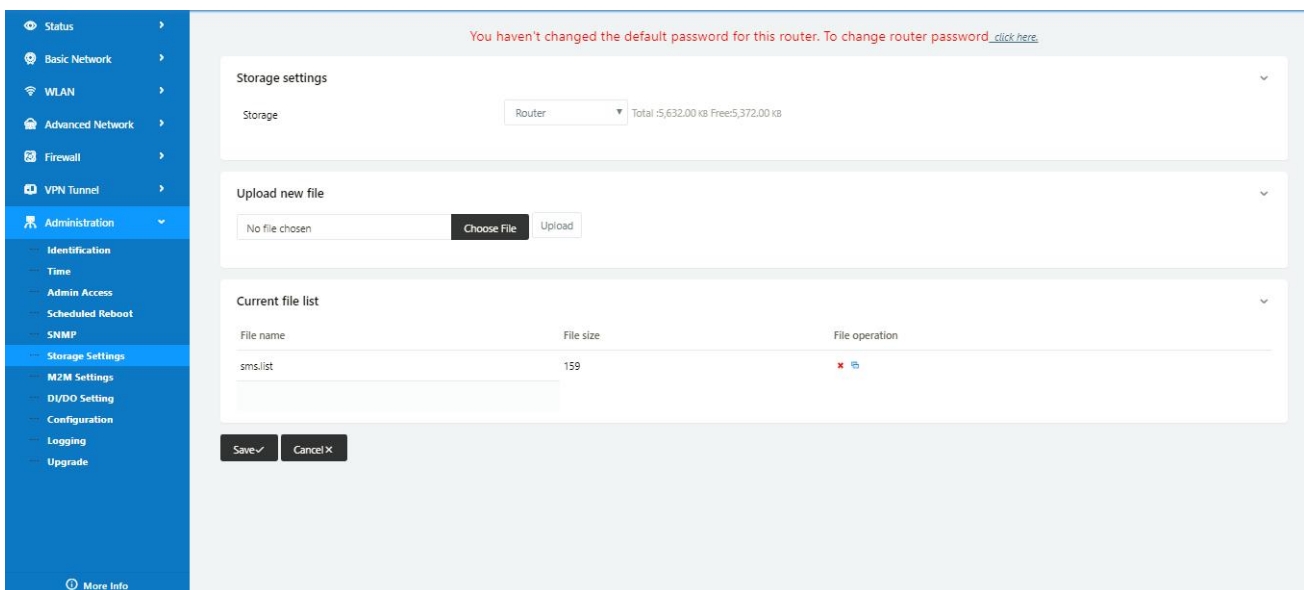
Please click “Advanced Network> Captive Portal” to check or modify the relevant parameter.



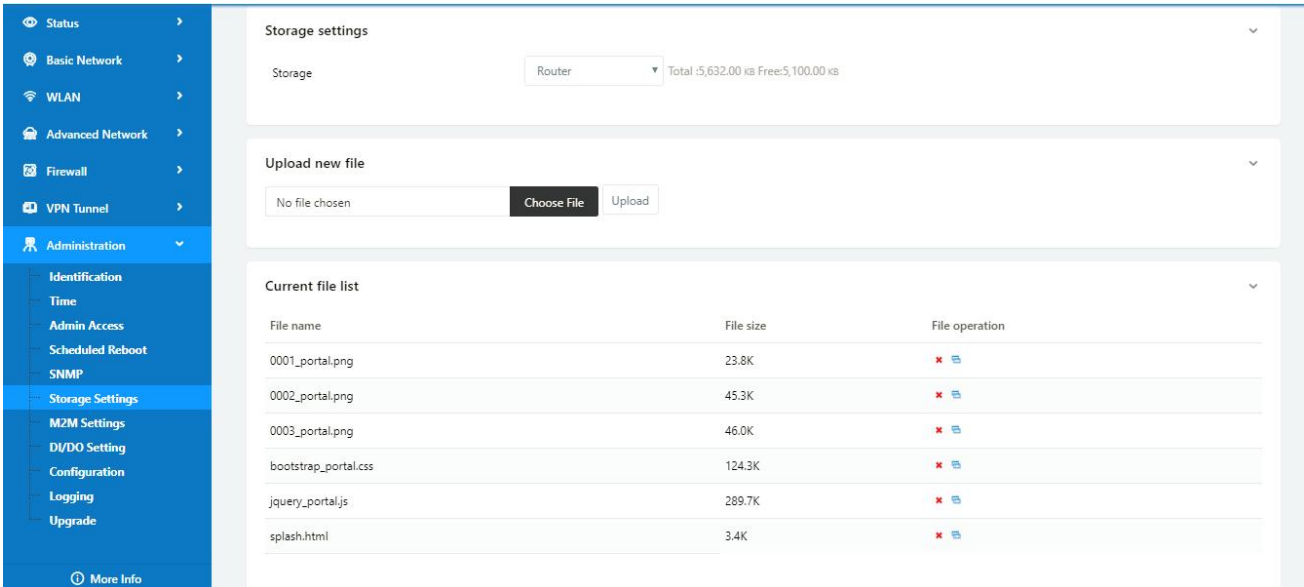
1) Upload Portal file and Splash.html by local

Upload portal images and splash.html in router for the Slider (0001_portal.png, 0002_portal.png, and 0003_portal.png) to the Router under the “Administration / Storage Settings” menu.

Furthermore, also might upload splash with images together.



Each Ad file just supports 3 Ad portal images. Picture format is acceptable for png/jpg and image size is less than 100Kbytes and resolution is 800*600. Picture name is 0001_portal.png, 0002_portal.png and 0003_portal.png. Furthermore, please keep image names the same between portal file and splash.html.



```

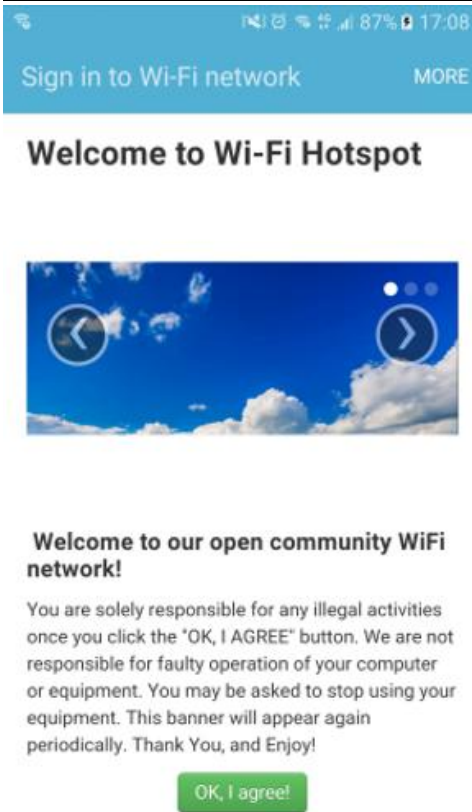
<!-- <hr> -->

<div id="myCarousel" class="carousel slide marketing">
  <ol class="carousel-indicators">
    <li data-target="#myCarousel" data-slide-to="0" class="active"></li>
    <li data-target="#myCarousel" data-slide-to="1"></li>
    <li data-target="#myCarousel" data-slide-to="2"></li>
  </ol>

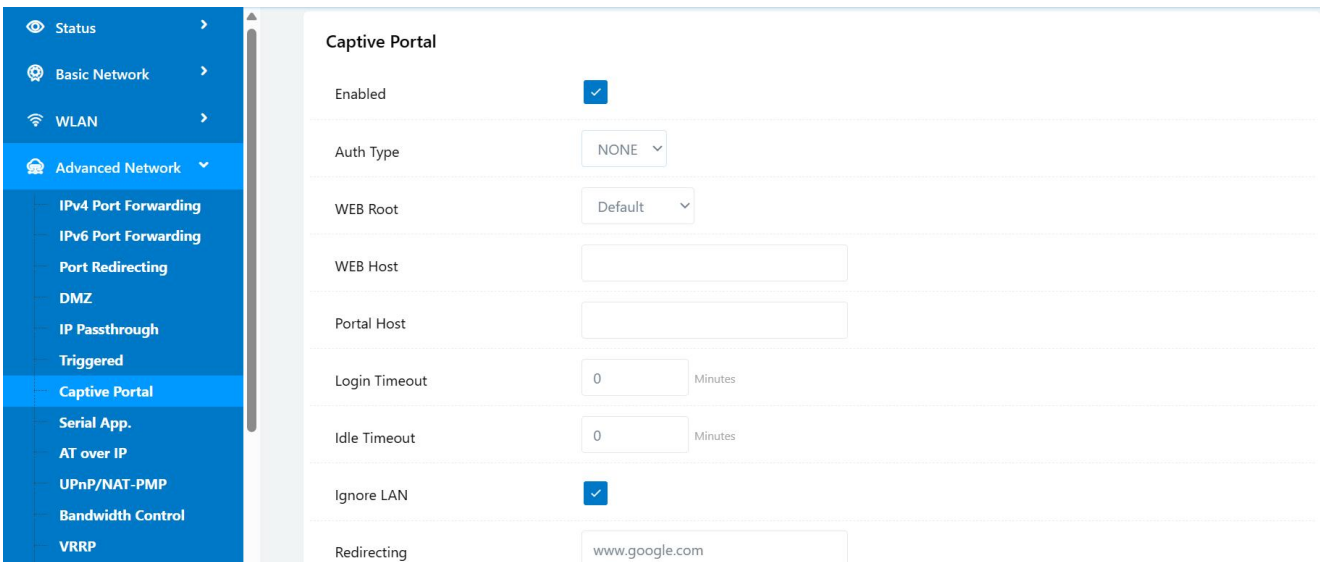
  <div class="carousel-inner">
    <div class="item active">
      
    </div>
    <div class="item">
      
    </div>
    <div class="item">
      
    </div>
  </div>
  <a class="left carousel-control" href="#myCarousel" data-slide="prev">&lsaquo;</a>
  <a class="right carousel-control" href="#myCarousel" data-slide="next">&rsaquo;</a>
</div>

<!-- <hr> -->
    
```

Finally, we can see the results by connect to router WIFI



2) Modify portal file storage path.
 Modify portal file storage for In-storage as below.



---End

3.8 GPS Settings

Please click “Advanced Network> GPS” to view or modify the relevant parameter.

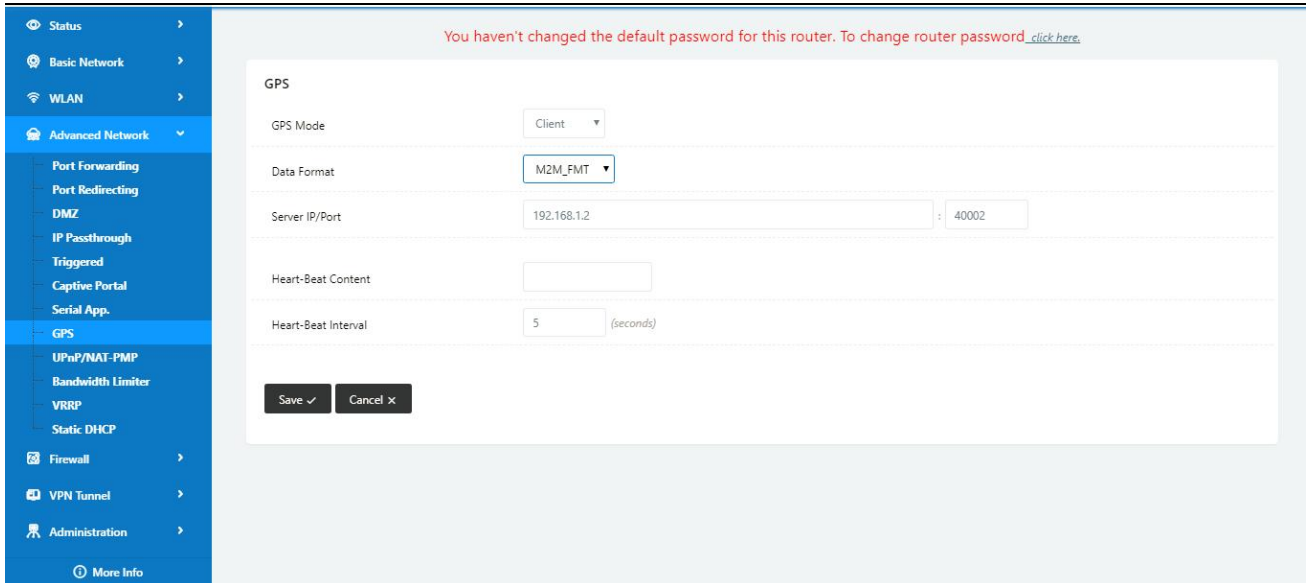


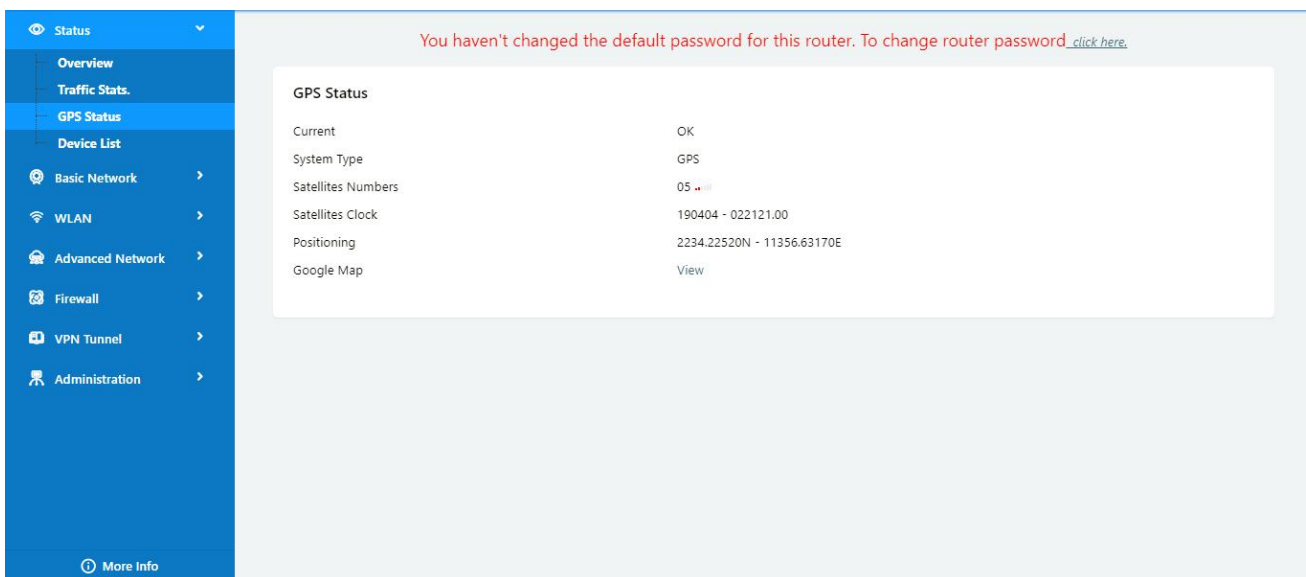
Table 4-6 “GPS” Instruction

parameter	Instruction	Default
GPS Mode	Enable/Disable	
GPS Format	NMEA and M2M_FMT(WLINK)	
Server IP/Port	GPS server IP and port	
Heartbeat	If choose M2M_FMT format, heart-beat ID will be packed into GPS data.	
Interval	GPS data transmit as the interval time.	

Step 1 Please click “save” to finis

Step 2 Connect the GPS antenna to router GPS interface

Step 3 Check GPS Status





M2M_FMT Format as below.

1. GPS data structure.

Router ID, gps_date, gps_time, gps_use, gps_latitude, gps_NS, gps_longitude, gps_EW, gps_speed, gps_degrees, gps_FS, gps_HDOP, gps_MSL

2. Example

0001_R081850ac,150904,043215.0,06,2234.248130,N,11356.626179,E,0.0,91.5,1,1.2,97.5

3. GPS data description

Field No.	Name	Format	Example	Description
1	Router ID	String	0001_R081850ac	0001 customizable product ID. _R router indicator. 081850ac Last 8digits of routers MAC address.
2	gps_date	yymmdd	150904	Date in year,month,day
3	gps_time	hhmmss.ss s	043215.0	UTC Time, Time of position fix.
4	gps_use	numeric	06	Satellites Used, Range 0 to 12.
5	gps_latitude	ddmm.mm mm	2234.248130	Latitude, Degrees + minutes.
6	gps_NS	character	N	N/S Indicator,N=north or S=south.
7	gps_longitude	ddmm.mm mm	11356.626179	Longitude, Degrees + minutes.
8	gps_EW	character	E	E/W indicator, E=east or W=west.
9	gps_speed	numeric	0.0	Speed(Knots) over ground, units is kn/h.
10	gps_degrees	numeric	91.5	Course over ground, unit is degree.
11	gps_FS	digit	1	Position Fix Status Indicator,
12	gps_HDOP	numeric	1.2	HDOP, Horizontal Dilution of Precision
13	gps_MSL	numeric	97.5	MSL Altitude, units is meter.

---End

3.9 Firewall

1) IP/MAC/Port Filtering

This part used to intercept packages from router's WAN/Celluar interface to Internet.

Test case:

1.1 Only allow three devices (MAC/LAN/WLAN) can access to Internet via WAN: 110.110.10.10

1.2 Only allow three devices (MAC/LAN/WLAN) can access to the router page (192.168.1.1)

On	Network Protocol	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>	IPv4	-	any/0	any/0	-	-	-	Drop	
<input checked="" type="checkbox"/>	IPv4	-	any/0	192.168.1.0/24	-	-	-	Accept	
<input checked="" type="checkbox"/>	IPv4	02:E1:8C:62:C4:01	any/0	any/0	-	-	-	Accept	
<input checked="" type="checkbox"/>	IPv4	00:FF:8F:5D:F7:82	any/0	any/0	-	-	-	Accept	
<input checked="" type="checkbox"/>	IPv4	00:90:9A:9A:B2:27	any/0	any/0	-	-	-	Accept	
<input checked="" type="checkbox"/>	IPv4	00:E1:8C:62:C4:05	any/0	any/0	-	-	-	Accept	

2) Key Word Filtering

This part used to filter key word packages from router's WAN/Celluar interface to Internet.

On	Key Word	Description
<input checked="" type="checkbox"/>	youtube	
<input checked="" type="checkbox"/>	facebook	

3) URL Filtering

This part used to filter URL from router's WAN/Celluar interface to Internet.

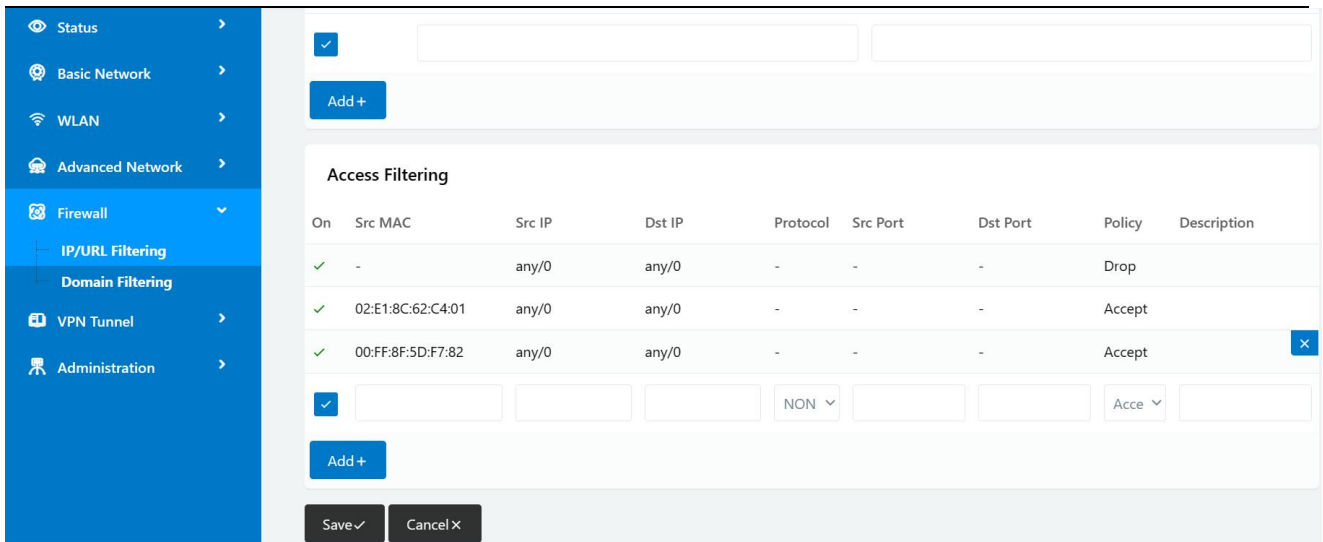
4) Access Filtering

This part used to filter packages from Internet to router's WAN/Celluar interface.

Test case:

4.1) Intercept all TCP packets accessing the router's WAN/Celluar(110.110.10.10).

4.2) Only two devices (MAC/LAN/WLAN) are allowed to be accessed from Internet packets.

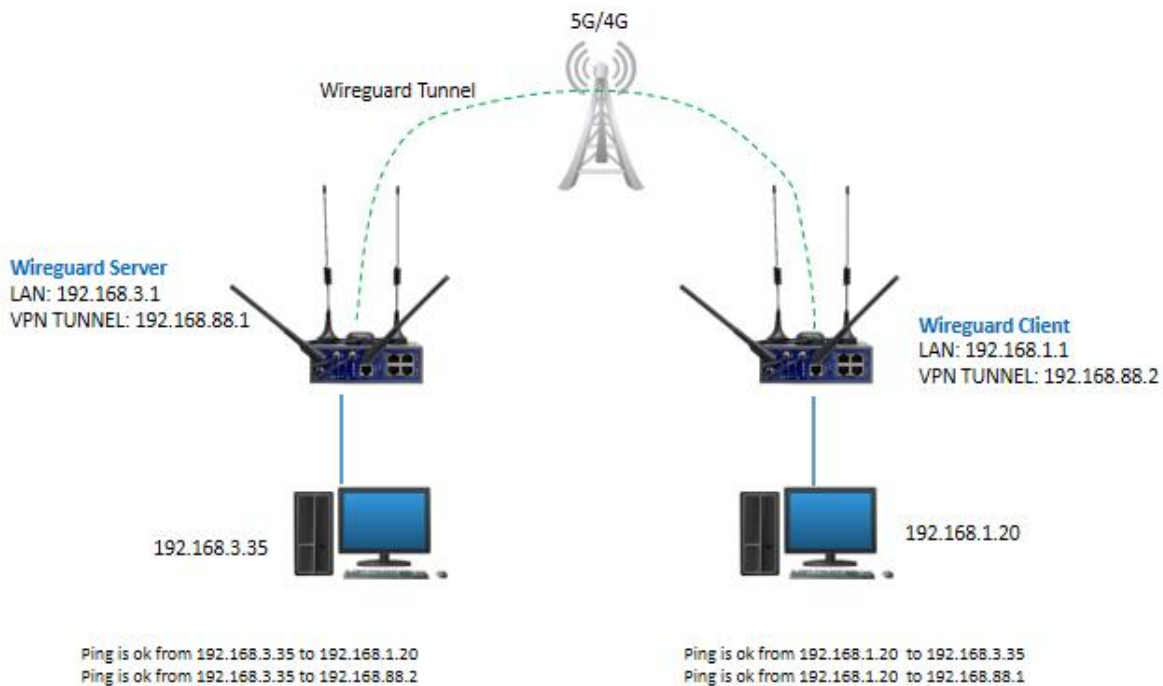


---End

3.10 VPN Tunnel

3.9.1 Wireguard

Wireguard VPN between two WL-Rxx Routers



1) Wireguard VPN Client Setting

Configure Wireguard Client as Server requested. Especially, the public Key and private key is generated by server or third party. Configure server public key in the peer key table and client private

key in the local key table.

Wireguard

Enabled

Mode Client

Peer IP/Port 113.87.81.122 : 51821

Local Key qFFPQ7MQL6G7mohLP3NYtvS5Zer05tDDdAFaFieJgUE=

Local IP/Mask 192.168.88.4/24 ex. 192.168.88.5/24

Peer Key 9VDgAnfn5xsNaKJ+Z6VKNCi5GSCpA+dkoscbXGKomkw=

Preshared Key

Peer Subnet IP/Mask 192.168.3.0/24 ex. 192.168.88.0/24

Save ✓ Cancel ✕

2) Wireguard Routing

There are two routings when Wireguard established.

Current Routing Table				
Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
default	192.168.10.1	0.0.0.0	0	wan
127.0.0.0	*	255.0.0.0	0	lo
192.168.1.0	*	255.255.255.0	0	lan
192.168.3.0	*	255.255.255.0	0	wg0
192.168.10.0	*	255.255.255.0	0	wan
192.168.10.1	*	255.255.255.255	0	wan
192.168.88.0	*	255.255.255.0	0	wg0

3) Wireguard Connection Check

Check VPN connection via Ping testing.

```

wg0      Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
         inet addr:192.168.88.2 P-t-P:192.168.88.2 Mask:255.255.255.0
         UP POINTOPOINT RUNNING NOARP MTU:1420 Metric:1
         RX packets:7 errors:0 dropped:0 overruns:0 frame:0
         TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:764 (764.0 B) TX bytes:820 (820.0 B)

root@Router:/tmp/home/root# ping 192.168.88.1
PING 192.168.88.1 (192.168.88.1): 56 data bytes
64 bytes from 192.168.88.1: seq=0 ttl=64 time=1.388 ms
64 bytes from 192.168.88.1: seq=1 ttl=64 time=1.181 ms
64 bytes from 192.168.88.1: seq=2 ttl=64 time=1.557 ms
64 bytes from 192.168.88.1: seq=3 ttl=64 time=1.246 ms
^C
--- 192.168.88.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.181/1.343/1.557 ms

root@Router:/tmp/home/root# ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1): 56 data bytes
64 bytes from 192.168.3.1: seq=0 ttl=64 time=1.375 ms
64 bytes from 192.168.3.1: seq=1 ttl=64 time=1.061 ms
64 bytes from 192.168.3.1: seq=2 ttl=64 time=1.141 ms
64 bytes from 192.168.3.1: seq=3 ttl=64 time=1.141 ms
^C
--- 192.168.3.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.061/1.179/1.375 ms

root@Router:/tmp/home/root# ping 192.168.3.35
PING 192.168.3.35 (192.168.3.35): 56 data bytes
64 bytes from 192.168.3.35: seq=0 ttl=63 time=2.570 ms
64 bytes from 192.168.3.35: seq=1 ttl=63 time=1.875 ms
64 bytes from 192.168.3.35: seq=2 ttl=63 time=2.015 ms
64 bytes from 192.168.3.35: seq=3 ttl=63 time=2.251 ms
^C
--- 192.168.3.35 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.875/2.177/2.570 ms
    
```

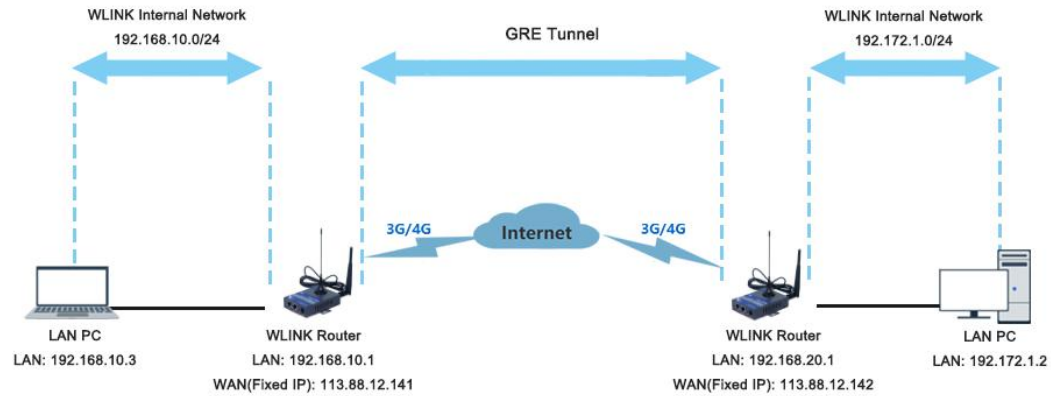
Wireguard Peer Virtual IP

WG Server Gateway IP

WG Server LAN Host IP

3.9.2 GRE

GRE Tunnel between two WL-Rxx Routers



- 1) WL-R200(A) Config
- Navigate to **Basic Network > LAN**.

This screenshot shows the LAN configuration page. A red warning message at the top states: "You haven't changed the default password for this router. To change router password [click here](#)." The LAN section contains a table with the following data:

Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)	DHCP Relay	DHCP Server Address
br0	192.168.10.1	255.255.255.0	✓	192.168.10.2 - 51	1440	✗	

Below the table is a form for adding a new LAN entry with fields for bridge, IP address, subnet mask, DHCP server, IP pool, lease time, DHCP relay, and DHCP server address. A blue "Add +" button is located below the form. The DNS section below has a checkbox for "Use Custom DNS" which is currently unchecked.

Navigate to VPN Tunnel > GRE

This screenshot shows the VPN Tunnel configuration page. The left sidebar is expanded to "VPN Tunnel" > "GRE". The GRE Tunnel section contains a table with the following data:

On	Idx	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
✓	1	192.168.10.10	113.113.11.11	113.113.10.10	✓	10	5	A

Below the table is a form for adding a new GRE tunnel with fields for On, Idx, Tunnel Address, Tunnel Source, Tunnel Destination, Keepalive, Interval, Retries, and Description. A blue "Add +" button is located below the form. The GRE Route section contains a table with the following data:

On	Tunnel Index	Destination Address	Default Route	Description
✓	1	192.172.1.0/24	✗	A

Below the table is a form for adding a new GRE route with fields for On, Tunnel Index, Destination Address, Default Route, and Description. A blue "Add +" button is located below the form. At the bottom of the page are "Save ✓" and "Cancel ✗" buttons.

2) WL-R200(B) Config

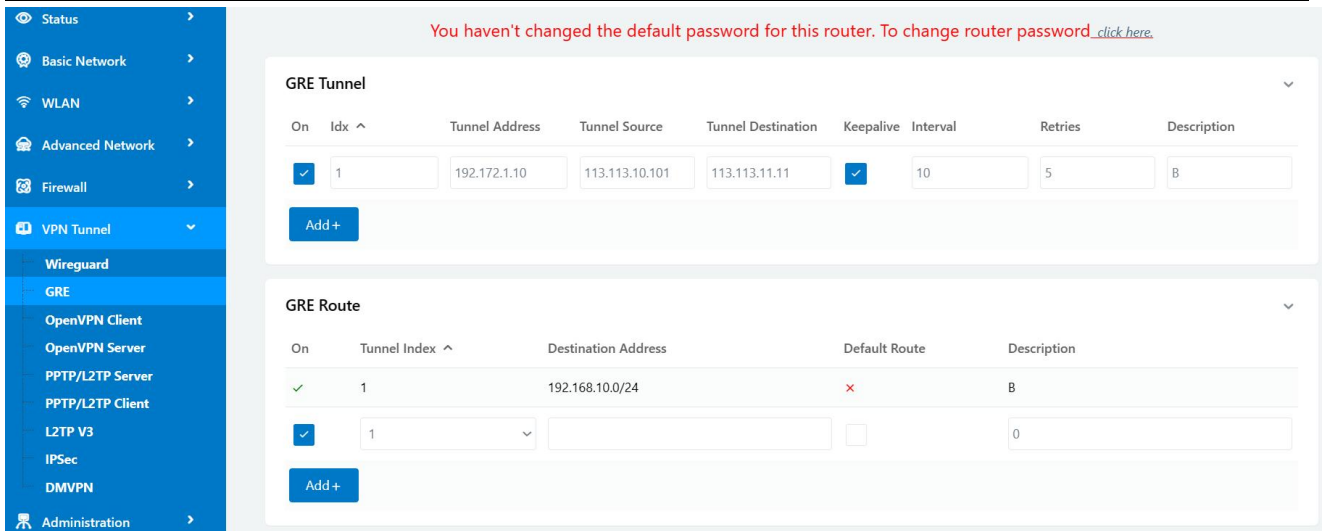
Navigate to Basic Network > LAN

This screenshot shows the LAN configuration page for the WL-R200(B) router. A red warning message at the top states: "You haven't changed the default password for this router. To change router password [click here](#)." The LAN section contains a table with the following data:

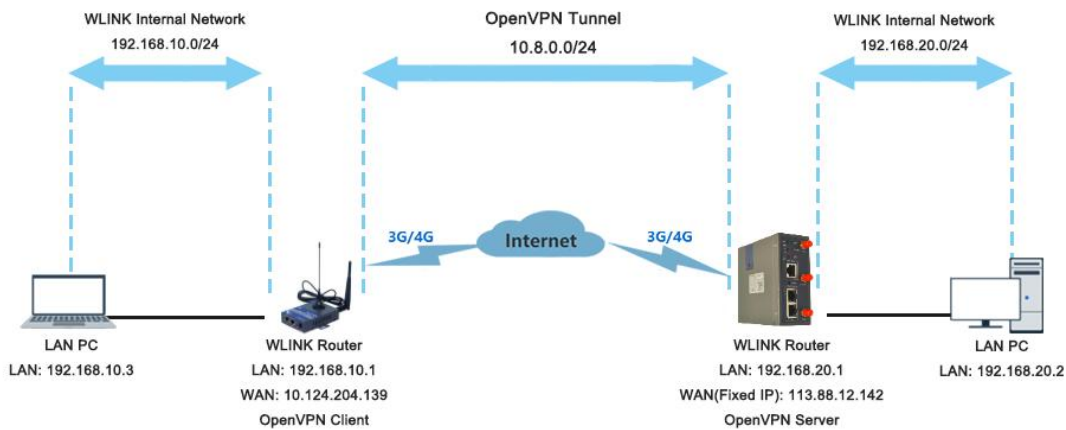
Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)	DHCP Relay	DHCP Server Address
br0	192.172.1.1	255.255.255.0	✓	192.172.1.2 - 51	1440	✗	

Below the table is a form for adding a new LAN entry with fields for bridge, IP address, subnet mask, DHCP server, IP pool, lease time, DHCP relay, and DHCP server address. A blue "Add +" button is located below the form. The DNS section below has a checkbox for "Use Custom DNS" which is currently unchecked.

Navigate to VPN Tunnel > GRE

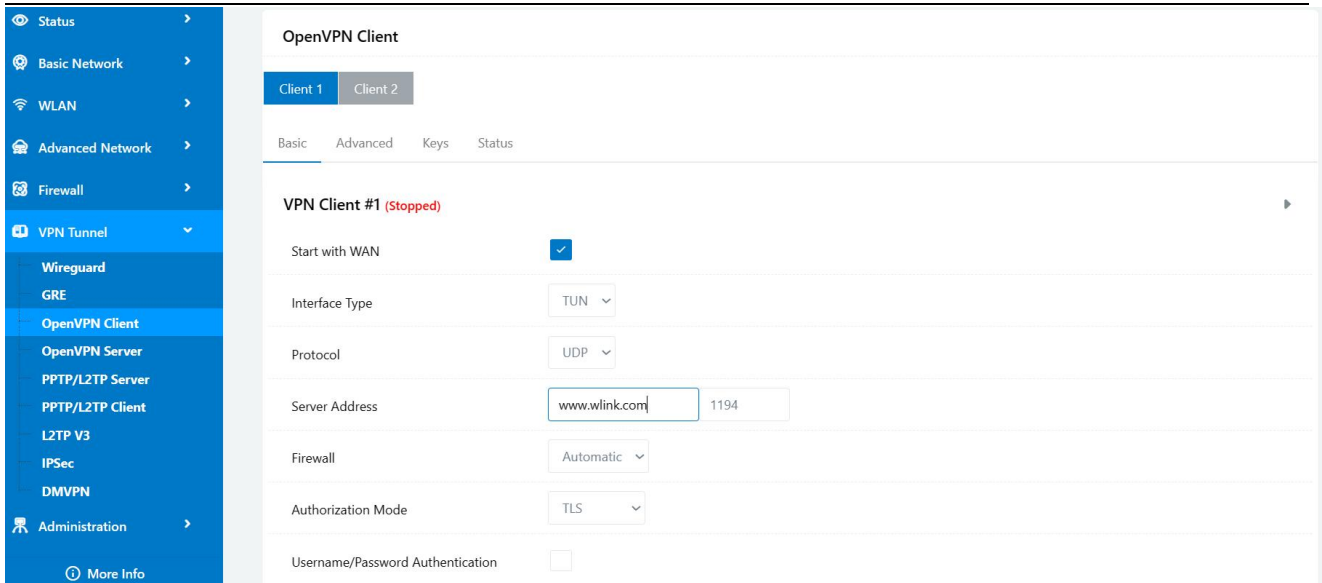


3.9.3 OpenVPN

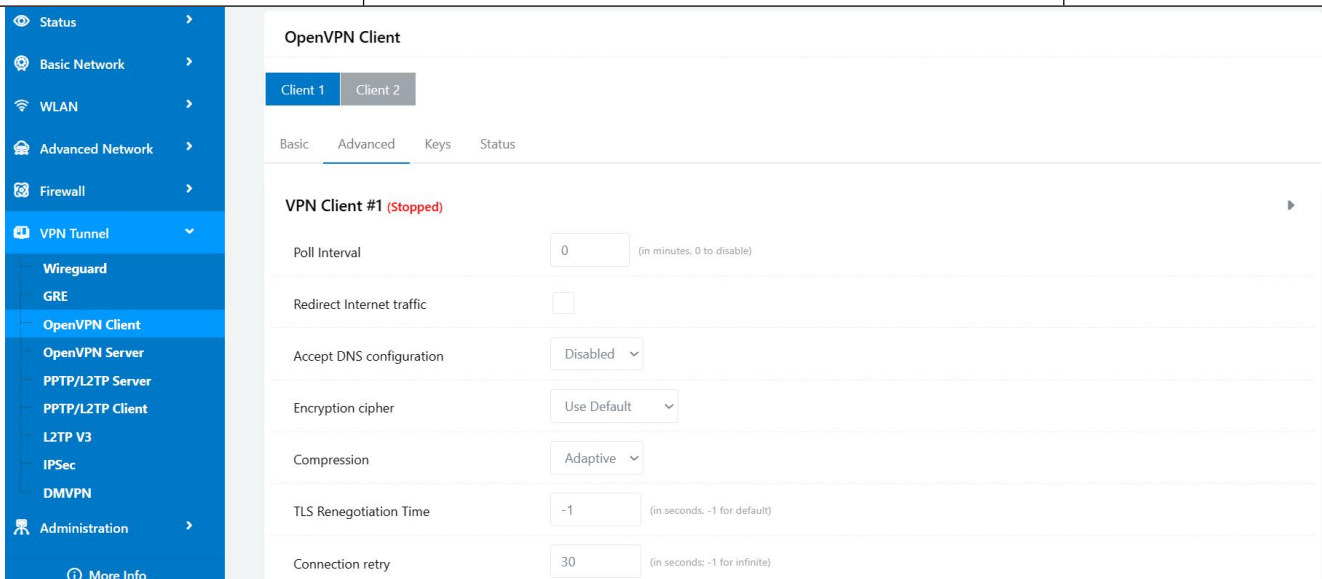


OpenVPN between WL-Rxx client and Server

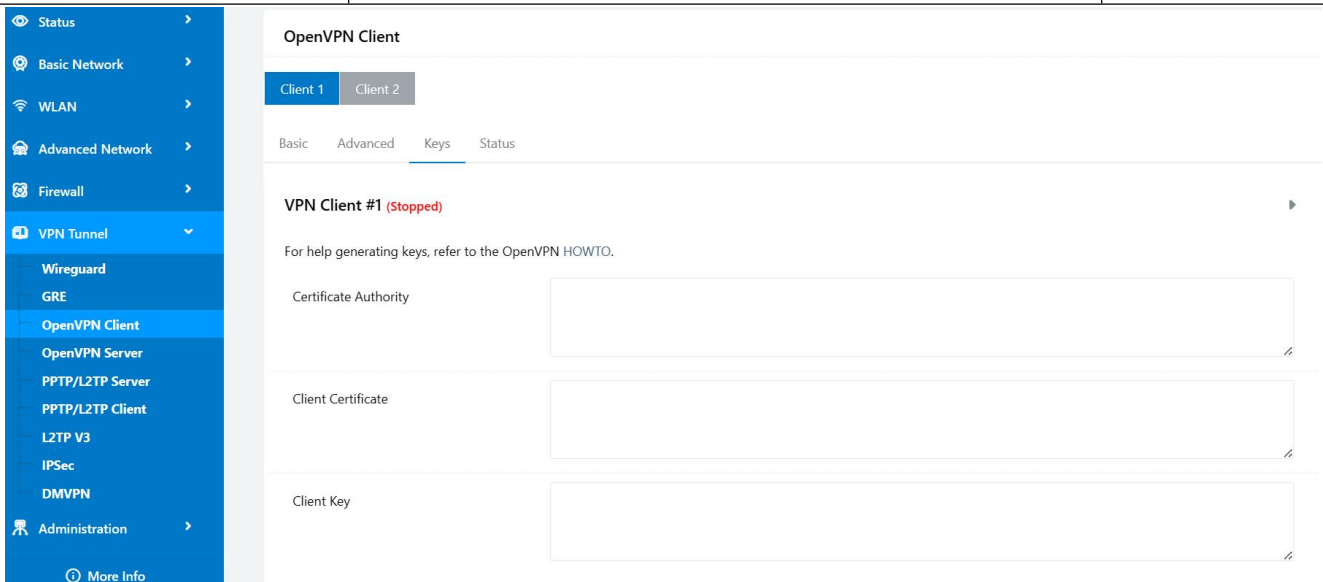
Please click "VPN Tunnel> OpenVPN Client" to check or modify the relevant parameter.



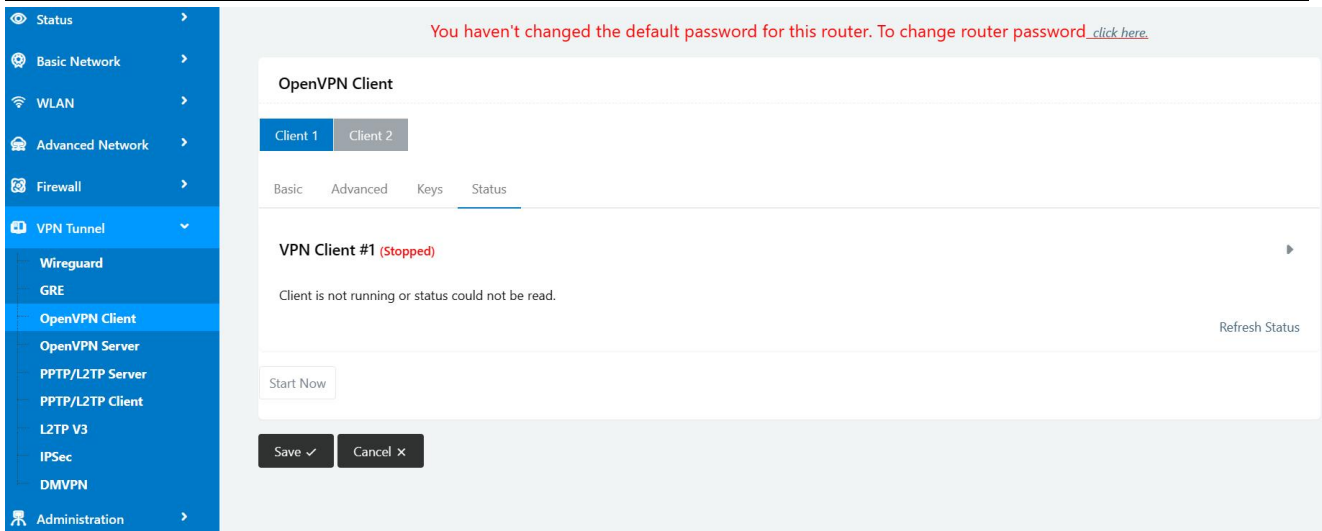
Parameter	Instruction	Default
Start with WAN	Enable the Openvpn feature for 4G/3G/WAN port.	
Interface Type	Tap and Tun type are optional. Tap is for bridge mode and Tunnel is for routing mode.	
Protocol	UDP and TCP optional.	
Server Address	The Openvpn server public IP address and port.	
Firewall	Auto, External only and Custom are optional	
Authorization Mode	TLS, Static key and Custom are optional.	
User name/Password Authentication	As the configuration requested.	
HMAC authorization	As the configuration requested.	
Create NAT on tunnel	Configure NAT in Openvpn tunnel.	



Parameter	Instruction	Default
Poll Interval	OpenVPN client check router's status as interval time.	
Redirect Internet Traffic	Configure OpenVPN as default routing.	
Access DNS	As the configuration requested.	
Encryption	As the configuration requested.	
Compression	As the configuration requested.	
TLS Renegotiation Time	TLS negotiation time. -1 as default for 60s.	
Connection Retry Time	OpenVPN retry to connection interval.	
Verify server certificate	As the configuration requested.	
Custom Configuration	As the configuration requested.	



Parameter	Instruction	Default
Certificate Authority	Keep certificate same as the server	
Client Certificate	Keep client certificate same as the server	
Client Key	Keep client key same as the server	



Parameter	Instruction	
Status	Check OpenVPN status and data statistics.	

Click “save” and “start now” to enable OpenVPN when you have done all the client config.



OpenVPN Keys Guide

The flowing steps are for server running on Windows 7/8/10

Access to (<http://openvpn.net/release/>) and download the file “openvpn-2.3.0-install.exe” (or higher)



Index of /release

Name	Last modified	Size	Description
Parent Directory		-	
lzo-1.08-3.0.el2.dag.i386.rpm	21-Feb-2012 00:50	55K	
lzo-1.08-3.0.rh7.dag.i386.rpm	21-Feb-2012 00:50	54K	
lzo-1.08-3.0.rh8.dag.i386.rpm	21-Feb-2012 00:50	58K	
lzo-1.08-4.0.rh9.rf.i386.rpm	21-Feb-2012 00:50	59K	
lzo-1.08-4.1.el3.rf.i386.rpm	21-Feb-2012 00:50	58K	
lzo-1.08-4.1.el3.rf.x86_64.rpm	21-Feb-2012 00:50	55K	
lzo-1.08-4.1.fc1.rf.i386.rpm	21-Feb-2012 00:50	58K	

After installing OpenVPN, please find the OpenVPN folder to generate the certificate of server and client. (Access to <http://openvpn.net> for more information)



PC > Newdisk (D:) > OpenVPN >

Name	Date modified	Type	Size
bin	2019-01-10 11:42	File folder	
config	2019-01-10 14:10	File folder	
doc	2019-01-10 11:42	File folder	
easy-rsa	2019-01-10 11:54	File folder	
log	2019-01-10 14:10	File folder	
sample-config	2019-01-10 11:41	File folder	
icon.ico	2015-02-18 17:56	Icon	22 KB
Uninstall.exe	2019-01-10 11:42	Application	117 KB

Configure "vas.bat.sample" to complete the initialization step and keys

This PC > Newdisk (D:) > OpenVPN > easy-rsa >

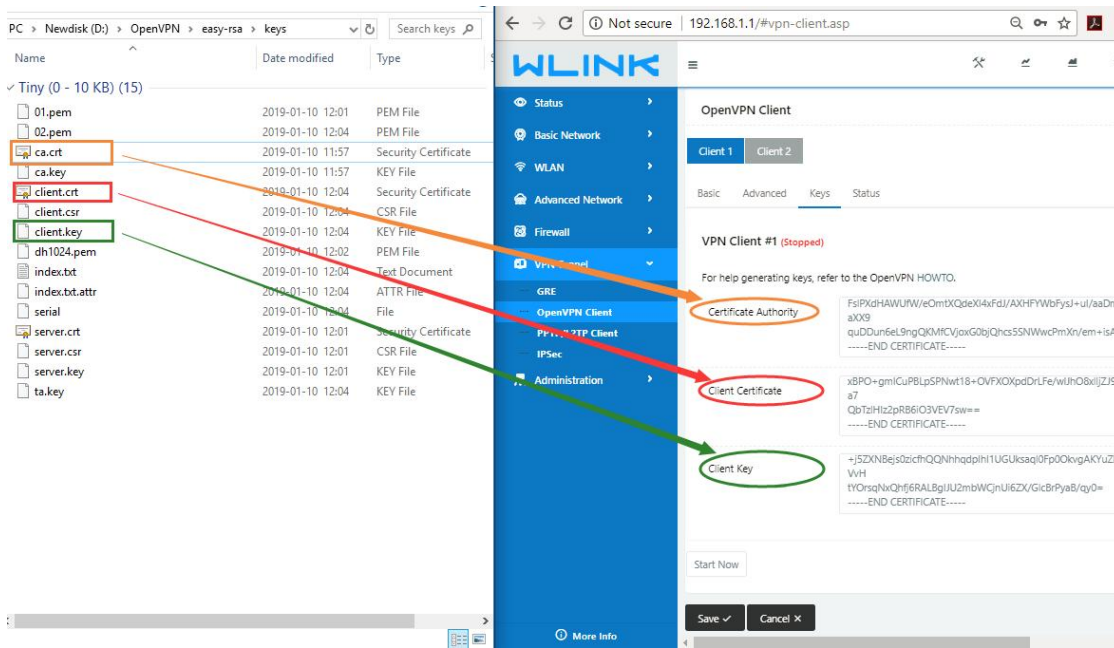
Name	Date modified	Type	Size
keys	2019-01-10 12:04	File folder	
.rnd	2019-01-10 12:04	RND File	1 KB
build-ca.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-dh.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key-pass.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key-pkcs12.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key-server.bat	2016-01-04 20:41	Windows Batch File	1 KB
clean-all.bat	2016-01-04 20:41	Windows Batch File	1 KB
index.bt.start	2016-01-04 20:41	START File	0 KB
init-config.bat	2016-01-04 20:41	Windows Batch File	1 KB
openssl-1.0.0.cnf	2016-01-04 20:41	CNF File	9 KB
README.txt	2016-01-04 20:41	Text Document	2 KB
revoke-full.bat	2016-01-04 20:41	Windows Batch File	1 KB
serial.start	2016-01-04 20:41	START File	1 KB
vars.bat	2019-01-10 11:43	Windows Batch File	1 KB
vars.bat.sample	2019-01-10 11:43	SAMPLE File	1 KB

Configure the client keys to WLINK OpenVPN client GUI when you create the server and client certificate in the path OpenVPN/easy-rsa/keys

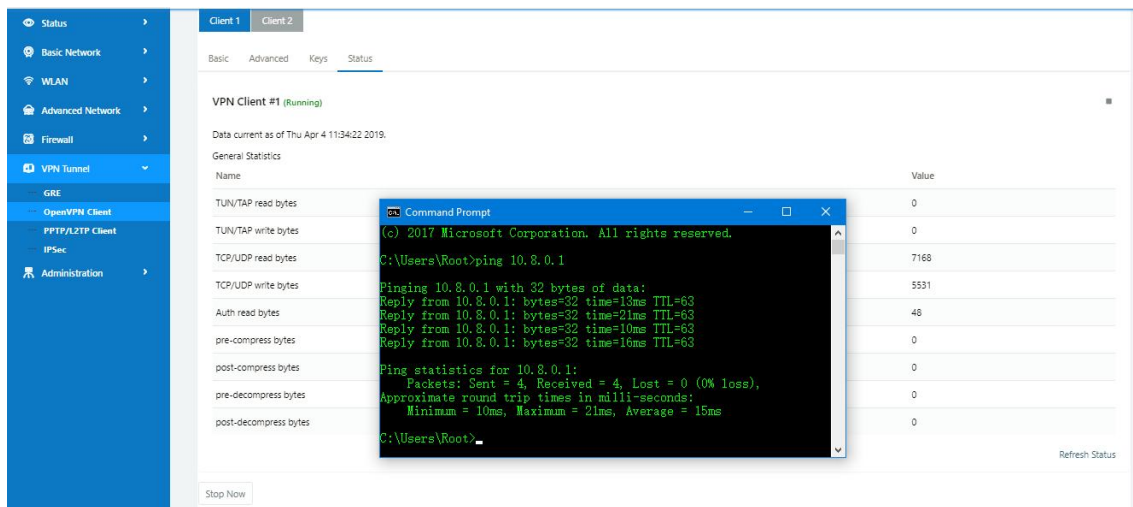
Client certificate (Generated on the server)

Name	Date modified	Type	Size
ca.crt	2019-01-10 11:57	Security Certificate	2 KB
client.crt	2019-01-10 12:04	Security Certificate	4 KB
client.key	2019-01-10 12:04	KEY File	1 KB
client.ovpn	2019-01-10 14:08	OpenVPN Config ...	4 KB
ta.key	2019-01-10 12:04	KEY File	1 KB

OpenVPN>easy-rsa>keys



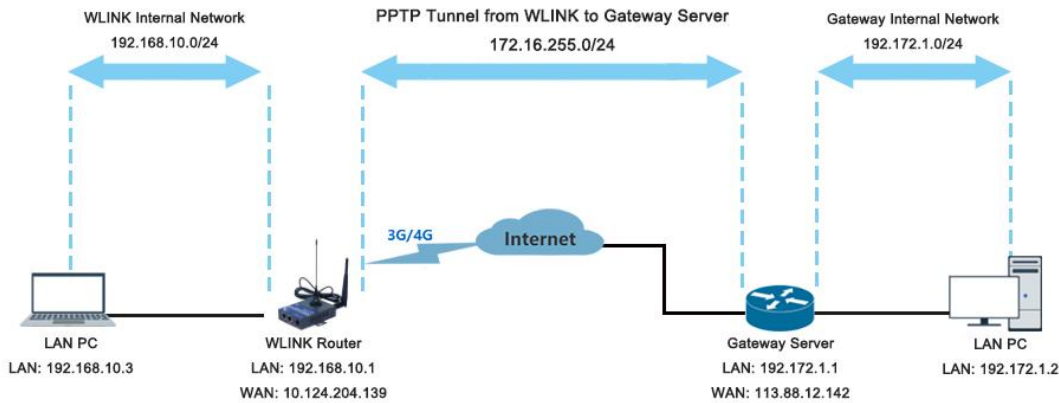
Ping test to your server when the tunnel is established



---End

3.9.4 L2TP/PPTP

Please click "VPN Tunnel>PPTP/L2TP Client" to view or modify the relevant parameter.



Configured as PPTP

- Status
- Basic Network
- WLAN
- Advanced Network
- Firewall
- VPN Tunnel
 - Wireguard
 - GRE
 - OpenVPN Client
 - OpenVPN Server
 - PPTP/L2TP Server
 - PPTP/L2TP Client
 - L2TP V3
 - IPSec
 - DMVPN
 - Administration
- More Info

L2TP/PPTP Basic

On	Protocol	Name	Server	Username	Password	Firewall	Default Route	Local IP
<input checked="" type="checkbox"/>	PPTP	3	wlinktech.com.cn	test123	test123	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

[Add +](#)

L2TP Advanced

On	Name	Accept DNS	MTU	MRU	Tunnel Auth	Tunnel Password	Custom Options
<input checked="" type="checkbox"/>		NO			<input type="checkbox"/>		

[Add +](#)

PPTP Advanced

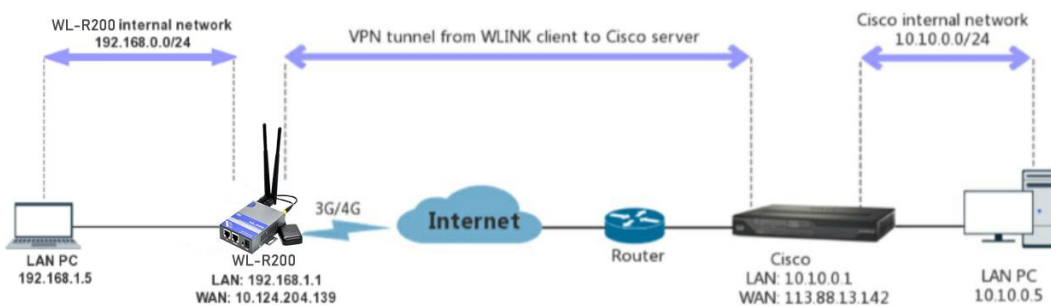
On	Name	Accept DNS	MTU	MRU	MPPE	MPPE Stateful	Custom Options
<input checked="" type="checkbox"/>	3	NO	1440	1440	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Note: The Custom Options are based on your server

---End

3.9.5 IPSec

IPSec between WL-R200 and Cisco Router



1) Cisco Config (main mode)

```

!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
crypto isakmp key test1234 address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set Tran-set esp-3des esp-sha-hmac
crypto ipsec nat-transparency spi-matching
!
    
```

2) WLINK Config

Navigate to VPN Tunnel > IPSec > Group Setup

The screenshot shows the 'IPSec' configuration page with the 'Group Setup' tab selected. The left sidebar contains navigation options: Status, Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel (selected), Wireguard, GRE, OpenVPN Client, OpenVPN Server, PPTP/L2TP Server, PPTP/L2TP Client, L2TP V3, IPSec (highlighted), DMVPN, and Administration. The main content area includes the following settings:

- Enable IPSec:
- IPSec Extensions: Normal
- Local Security Gateway Interface: Cellular
- Local Security Group Subnet/Netmask: 192.168.1.0/24 (example: 192.168.1.0/24)
- Local Security Firewalling:
- Remote Security Gateway IP/Domain: 113.88.13.142
- Remote Security Group Subnet/Netmask: 10.0.0.0/24 (example: 192.168.88.0/24)
- Remote Security Firewalling:

Navigate to VPN Tunnel > IPSec > Basic Setup

The screenshot shows the 'IPSec' configuration page with the 'Basic Setup' tab selected. The left sidebar is the same as in the previous screenshot. The main content area includes the following settings:

- Keying Mode: IKE
- Auth Mode: Preshared Key
- Phase 1 DH Group: Group 2 - modp1024
- Phase 1 Encryption: 3DES (168-bit)
- Phase 1 Authentication: MD5 HMAC (96-bit)
- Phase 1 SA Life Time: 28800 seconds
- Phase 2 DH Group: Group 2 - modp1024
- Phase 2 Encryption: 3DES (168-bit)
- Phase 2 Authentication: MD5 HMAC (96-bit)
- Phase 2 SA Life Time: 3600 seconds
- Preshared Key: *****

Navigate to VPN Tunnel > IPSec > Advanced Setup

VPN Status



IPSec 1 Connected

Phase 1
 Status 36 minutes

Phase 1 IKE 3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024

Phase 2
 Status TUNNEL

Phase 2 ESP 3DES_CBC/HMAC_MD5_96/MODP_1024

IPSec Recv. 5700 Bytes

IPSec Send. 6120 Bytes

---End